Chapitre 1

Anneaux et idéaux

1.1 Définitions et premières propriétés

Définition 1.0.1. On appelle anneau commutatif unitaire un groupe abélien $(A, +)$ muni d'une opération de multiplication $(a, b) \to ab$ vérifiant les propriétés suivantes :

1. il existe un élément $1 \in A$ tel que pour tout $a \in A$, $1a = a$ (élément neutre pour la multiplication).
2. pour tous $a, b, c \in A$, on a $a(bc) = (ab)c$ (associativité).
3. pour tous $a, b, c \in A$, on a $a(b + c) = ab + ac$ (distributivité).
4. pour tous $a, b \in A$, on a $ab = ba$ (commutativité).

Dans tout ce qui suit, A est un anneau commutatif et unitaire avec $0 \neq 1$.

Remarques 1.0.1.

1. Si $a \in A$ et si n est un entier positif ou nul, on définit par récurrence a^n, en posant $a^0 = 1$ et $a^n = a(a^{n-1})$.
2. L'élément neutre pour la multiplication 1_A est unique.
3. pour tout $a \in A$, on a $(-1)a = -a$.
4. pour tout $a \in A$ et pour tous entiers $m, n \geq 0$, on a $a^{m+n} = a^m a^n$.
5. pour tout $a, b \in A$ et tout entier $n \geq 0$ on a (la formule du binôme)

$$(a + b)^n = \sum_{k=0}^{n} C_n^k a^k b^{n-k}.$$

Définition 1.0.2. Un élément $a \in A$ est dit inversible s'il existe $b \in A$ tel que $ab = 1$. Cet élément est unique et appelé l'inverse de a. Il est généralement noté a^{-1}.
L'ensemble des éléments inversibles d'un anneau est noté $U(A)$.

Scanned with CamScanner

Proposition 1.1

L'ensemble $U(A)$ est un groupe multiplicatif.

Démonstration. Observons d'abord que la multiplication définit une loi interne. En effet, si $a, b \in U(A)$ alors $(ab)(a^{-1}b^{-1}) = (aa^{-1})(bb^{-1}) = 1$. Ainsi ab est aussi inversible (est d'inverse $a^{-1}b^{-1}$). Maintenant il est clair que 1 est l'élément neutre pour cette loi et pour $a \in U(A)$ l'élément a^{-1} est son inverse. □

Définition 1.1.1. Soit $a \in A$. On dit que a est un diviseur de zéro s'il existe un élément $b \in A - \{0\}$, tel que $ab = 0$. Un anneau A est dit intègre s'il n'a pas de diviseur de zéro autre que l'élément 0. Ainsi, un anneau A est intègre si et seulement si pour tous $a, b \in A$, $ab = 0$ implique $a = 0$ ou $b = 0$.

Définition 1.1.2. On dira que l'anneau A est un corps si tout élément non nul de A est inversible (c-à-d, $U(A) = A - \{0\}$).

***Exemples* 1.1.1.**

1. L'anneau $\mathbb{Z}$ est intègre et $U(\mathbb{Z}) = \{1, -1\}$.
2. Dans $\mathbb{R}$ tout élément non nul est inversible. C'est donc un corps.

1.2 Morphismes d'anneaux

Définition 1.1.3. Soient A et B deux anneaux. Une application $f : A \to B$ est dite homomorphisme d'anneaux (ou simplement un morphisme d'anneaux) si

1. $f(0_A) = 0_B$ et $f(1_A) = 1_B$.
2. pour tous $a, b \in A$, $f(a + b) = f(a) + f(b)$ et $f(ab) = f(a)f(b)$.

En plus, si f est bijective on dit que f est un isomorphisme d'anneaux et que A et B sont deux anneaux isomorphes.

Remarque 1.1.1. Soit $f : A \to B$ un morphisme d'anneaux. Si $a \in U(A)$ alors $f(a) \in U(B)$. En effet, $f(a)f(a^{-1}) = f(aa^{-1}) = f(1_A) = 1_B$.

Définition 1.1.4. Soit A un anneau. On dira qu'une partie $B \subseteq A$ est un sous-anneau si B contient les éléments 0_A et 1_A et si B est stable par addition, multiplication et stable par opposé.

Remarques 1.1.1.

1. Soit A un anneau. Tout sous-anneau B de A est aussi un anneau avec $0_B = 0_A$ et $1_B = 1_A$.
2. Si $f : A \to B$ est un morphisme d'anneaux, alors l'image de f

$$\mathrm{Im}(f) = f(A) = \{f(a) \mid a \in A\}$$

Scanned with CamScanner

- est un sous-anneau de B.

1.3 Anneaux de polynômes

Définition 1.1.5. Soit A un anneau et X une indéterminée.

— On appelle P polynôme à une indéterminée X et à coefficients dans A toute somme finie de la forme

$$P := P(X) = a_0 + a_1X + a_2X^2 + ... + a_nX^n = \sum_{k=0}^{n} a_kX^k$$

avec $a_0, \cdots, a_n \in A$. Les scalaires $a_0, ..., a_n$ sont appelés les coefficients de P.

— On note $A[X]$ l'ensemble des polynômes à une indéterminée et à coefficients dans A.

— Le polynôme nul 0 est le polynôme dont tous les coefficients sont nuls.

— On dit que deux polynômes sont égaux si et seulement si les coefficients de même ordre dans P et dans Q sont égaux.

L'ensemble $A[X]$ muni de l'addition et de la multiplication usuelles (comme dans $\mathbb{R}[X]$ et $\mathbb{C}[X]$) est un anneau commutatif unitaire.

Définition 1.1.6 (Degré d'un polynôme)**.** Soient A un anneau et $P = \sum_{k=0}^{n} a_kX^k \in A[X]$. On définit le degré de P, noté $\deg P$, par

— Si $P = 0$, on pose $\deg P = -\infty$

— Si $P \neq 0$, alors $\deg P = \max\{k \in \mathbb{N} \mid a_k \neq 0\}$.

Proposition 1.2

Soient $P, Q \in A[X]$ non nuls. Alors,

1. $\deg(P + Q) \leq \max(\deg P, \deg Q)$. L'inégalité est stricte si et seulement si $\deg P = \deg Q$ et si les coefficients dominants de P et Q sont opposés.
2. $\deg(PQ) \leq \deg P + \deg Q$. En particulier, si A est intègre alors $\deg(PQ) = \deg P + \deg Q$.

Démonstration. On pose $P = \sum_{k=0}^{n} a_kX^k$ et $Q = \sum_{k=0}^{m} b_kX^k$ avec $\deg P = n$ et $\deg Q = m$ (donc $a_n \neq 0$ et $b_m \neq 0$).

(1) Si $n = m$, il est clair que $P + Q = \sum_{k=0}^{n}(a_k + b_k)X^k$. Donc, $\deg(P + Q) \leq n$ avec égalité si $a_n + b_n \neq 0$.

Scanned with CamScanner

Si $n > m$, on a :

$$P + Q = a_n X^n + ... + a_{m+1} X^{m+1} + \sum_{k=0}^{m} (a_k + b_k) X^k$$

Ainsi, $\deg(P + Q) = n = \max\{n, m\}$. De même, si $m > n$, $\deg(P + Q) = m = \max\{n, m\}$.

(2) Il suffit de remarquer que

$$PQ = \sum_{k=0}^{n+m} c_k X^k, \text{ où } \forall k \quad a_k = \sum_{i=0}^{k} a_i b_{k-i} = \sum_{i+j=k} a_i b_j.$$

Dans le cas où A est intègre, on a $c_{n+m} = a_n b_m \neq 0$ car $a_n \neq 0$ et $b_m \neq 0$. □

Proposition 1.3

Soit A un anneau intègre. Alors $U(A[X]) = U(A)$.

Démonstration. L'inclusion $U(A) \subseteq U(A[X])$ est clair. Prenons maintenant $P \in U(A[X])$. Il existe $Q \in A[X]$ tel que $PQ = 1$. Donc, $0 = \deg(PQ) = \deg(P) + \deg(Q)$. Ainsi, $\deg(P) = \deg(Q) = 0$. Par suite, $P, Q \in A$ et donc $P \in U(A)$. Enfin, $U(A[X]) \subseteq U(A)$. D'où l'égalité. □

Proposition 1.4

Si A est intègre, $A[X]$ est encore intègre.

Démonstration. Soient $P, Q \in A[X]$ tels que $PQ = 0$. Supposons que $P \neq 0$ et $Q \neq 0$. Alors, $\deg(PQ) = \deg(P) + \deg(Q) \geq 0$, ce qu'est absurde car $PQ = 0$ et donc $\deg(PQ) = -\infty$. □

1.4 Idéaux d'un anneau

Définition 1.4.1. Soit A un anneau. Un sous-ensemble non vide I de A est dit idéal de A si

- pour tous $x, y \in I$, $x + y \in I$.
- pour tout $a \in A$ et tout $x \in I$, on a $ax \in I$.

Remarque 1.4.1. Un ideal I de A contient toujours 0. En effet, I est non vide. Donc, pour $x \in I$, on a $0 = 0x \in I$. En plus pour tout $x \in I$, $-x = (-1)x \in I$.

***Exemples* 1.4.1.** Soit A un anneau.

1. A a deux ideaux naturels : l'idéal nul $\{0\}$ et l'anneau A lui même.

Scanned with CamScanner

2. Si $x \in A$, l'ensemble
$$(x) = \{ax \mid a \in A\}$$
est un idéal de A. Un tel idéal est dit principal de A engendré par x.

Définition 1.4.2. Soient A un anneau et $x_1, \cdots, x_n \in A$. L'ensemble
$$(x_1, \cdots, x_n) = \{a_1x_1 + \cdots + a_nx_n \mid a_1, \cdots, a_n \in A\}$$
est un ideal de A appelé l'idéal de type fini engendré par $x_1, \cdots, x_n$.
En particulier, l'idéal principal (x) avec $x \in A$ est un idéal de type fini engendré par x.

1.5 Opérations sur les idéaux

On peut effectuer plusieurs opérations sur les idéaux comme par exemple prendre leur intersection, somme ou produit.

Proposition 1.5

Si I et J sont deux idéaux de A, l'intersection $I \cap J$ est encore un idéal de A. Plus généralement, l'intersection d'une famille non vide d'idéaux est encore un idéal.

Démonstration. Remarquons d'abord que $I \cap J$ est non vide. En effet $0 \in I \cap J$. Pour tous $x, y \in I \cap J$ et tout $a \in A$, on a $x, y \in I$ et $x, y \in J$. Donc, $x + y \in I$, $x + y \in J$, $ax \in I$ et $ax \in J$. Donc, $x + y \in I \cap J$ et $ax \in I \cap J$. Par suite, $I \cap J$ est un idéal de A. □

Définition 1.5.1. Soient I et J deux idéaux d'un anneau A.

1. La somme de I et J est l'ensemble $I + J = \{x + y \mid x \in I \text{ et } y \in J\}$.
2. Le produit de I et J est l'ensemble $IJ = \{\Sigma_{fini} x_i y j \mid x_i \in I \text{ et } y_j \in J\}$.

Proposition 1.6

Soient I et J deux idéaux d'un anneau A. Alors, $I + J$ et IJ sont des idéaux de A.

Démonstration. Notons que $I + J$ et IJ sont non vides. En effet, ils contiennent au moins 0.
Soient $x, y \in I + J$ et $a \in A$. Donc, $x = x_1 + x_2$ et $y = y_1 + y_2$ avec $x_1, y_1 \in I$ et $x_2, y_2 \in J$. Donc, $x_1 + y_1 \in I$ et $x_2 + y_2 \in J$. Ainsi, $x + y = (x_1 + y_1) + (x_2 + y_2) \in I + J$ et $ax = ax_1 + ax_2 \in I + J$ (car $ax_1 \in I$ et $ax_2 \in J$).
La démonstration du fait que IJ est un idéal est laissée au lecteur comme exercice. □

Définition 1.6.1. Soient I et J deux idéaux d'un anneau A. Si $I + J = A$ alors I et J sond dits étrangers ou comaximaux.

Scanned with CamScanner

Proposition 1.7

Soit A un anneau. Soient I et J deux idéaux de A. Alors $IJ \subseteq I \cap J$. De plus, si I et J sont étrangers, alors on a égalité $IJ = I \cap J$.

Démonstration. Montrons la première assertion. Si $x \in I$ et $y \in J$, le produit xy appartient à la fois à I et à J. Par conséquent, $xy \in I \cap J$. Ainsi l'idéal IJ, qui est engendré par ces produits, est contenu dans $I \cap J$.
Pour la seconde assertion, on observe que si $I + J = A$, alors il existe $x \in I$ et $y \in J$ tels que $x + y = 1$. Soit $z \in I \cap J$ et écrivons

$$z = z1 = z(x + y) = zx + zy.$$

Comme $z \in J$ et $x \in I$, $zx \in IJ$. De même, $zy \in IJ$. Par conséquent, $zx + zy \in IJ$ et donc $z \in IJ$, d'où $I \cap J \subseteq IJ$. □

1.6 Idéaux et morphismes d'anneaux

Définition 1.7.1. Soit $f : A \to B$ un morphisme d'anneaux. On appelle noyau de f et l'on note $\ker f$ l'ensemble

$$\ker f = \{x \in A \mid f(x) = 0\}.$$

Proposition 1.8

Soient $f : A \to B$ un morphisme d'anneaux et J un idéal de B. Alors l'image réciproque

$$I = f^{-1}(J) = \{a \in A \mid f(a) \in J\}$$

est un idéal de A.

Démonstration. On a $f(0) = 0 \in J$. Donc, $0 \in J$. Soient $x, y \in I$ et $a \in A$. Alors, $f(x), f(y) \in J$, et donc $f(x+y) = f(x) + f(y) \in J$ et $f(ax) = f(a)f(x) \in J$. D'où, $x + y \in I$ et $ax \in I$. Par suite, I est un idéal de A. □

Remarque 1.8.1. L'image d'un idéal par un morphisme d'anneaux $f : A \to B$ n'est pas forcément un idéal dans B. Par exemple, pour le morphisme d'anneaux $f : \mathbb{Z} \to \mathbb{Q}$ défini par l'injection, l'image de $(2) = 2\mathbb{Z}$ l'idéal de $\mathbb{Z}$ engendré par 2 n'est pas un idéal de $\mathbb{Q}$. En effet $\frac{1}{3}.2 = \frac{2}{3} \notin f(2\mathbb{Z}) = 2\mathbb{Z}$.

Scanned with CamScanner

Corollaire 1.9

Soit $f : A \to B$ un morphisme d'anneaux. Alors $\ker(f)$ est un idéal de A.

Démonstration. Découle de la proposition précédente. En effet, $\ker(f) = f^{-1}\big(\{0\}\big)$. □

Définition 1.9.1. Soit A un anneau et I un idéal de A. Alors la relation $\sim$ definie sur $A \times A$ par $x \sim y \Leftrightarrow x - y \in I$ est une relation d'équivalence. L'ensemble des classes d'équivalences $A/\sim$ peut être muni d'une structure d'anneau pour les deux lois suivantes :

$$\overline{x} + \overline{y} = \overline{x+y} \qquad \text{et} \qquad \overline{x}.\overline{y} = \overline{x.y}$$

L'anneau $A/\sim$ est appelé anneau quotient de A par I et est noté A/I.
L'application $\pi : A \to A/I$ définie par $\pi(x) = \overline{x}$ est un morphisme d'anneaux appelé surjection canonique.

Proposition 1.10

Soient A un anneau et I un idéal de A. Les idéaux de A/I sont exactement les ensembles

$$J/I = \{\overline{x} \mid x \in J\}$$

avec J un idéal de A contenant I.

Démonstration. Soit K un ideal de A/I. Posons $J = \{x \in A \mid \overline{x} \in K\}$. Comme $\overline{0} \in K$ et $\overline{x} = \overline{0}$ pour tout $x \in I$, alors $I \subseteq J$. En plus, pour tous $x, y \in J$ et $a \in A$, on a $\overline{x+y} = \overline{x} + \overline{y} \in K$ et $\overline{ax} = \overline{a}.\overline{x} \in K$. Donc, $x + y \in J$ et $ax \in J$. Donc, J est un ideal de A contenant I et $J/I = K$.
Inversement, si J est idéal de A contenant I, alors il est facile de voir que J/I est idéal de A/I. □

Théoreme 1.11 (Premier théorème d'isomorphisme)

Soit $f : A \to B$ un morphisme d'anneaux. Alors, $A/\ker(f) \cong \mathrm{Im}(f)$.

Démonstration. On considère l'application $\overline{f} : A/\ker(f) \to \mathrm{Im}(f)$ définie par $\overline{f}(\overline{x}) = f(x)$.
Cette application est bien définie. En effet si $\overline{x} = \overline{y}$ alors $x - y \in \ker(f)$ et donc $f(x) - f(y) = f(x-y) = 0$. Ainsi, $f(x) = f(y)$. C'est à dire $\overline{f(x)} = \overline{f}(\overline{y})$.
Maintentant, il est facile de vérifier que $\overline{f}$ est un morphisme d'anneaux. En plus, $\overline{f}(\overline{x}) = 0$ si et seulement si $f(x) = 0$ si et seulement si $x \in \ker(f)$ si et seulement si $\overline{x} = \overline{0}$. Par suite,

Scanned with CamScanner

$\overline{f}$ est injective.
Aussi, pour tout $f(x) \in \mathrm{Im}(f)$, on a $f(x) = \overline{f}(\overline{x})$, et donc $\overline{f}$ est surjective. Enfin, $\overline{f}$ est bijective. □

Théoreme 1.12 (Deuxième théorème d'isomorphisme)

Soient $I \subseteq J$ deux idéaux d'un anneau A. Alors,

$$\frac{A/I}{J/I} \cong A/J$$

.

Démonstration. On considère l'application $f : A/I \to A/J$ définie par $f(\overline{x}) = \hat{x}$. Cette application est bien définie. En effet, $\overline{x} = \overline{y}$ implique que $x - y \in I \subseteq J$ et donc $\hat{x} = \hat{y}$. Par suite, $f(\overline{x}) = f(\overline{y})$.
Il est trivial de vérifier que f est un morphisme d'anneaux. Ensuite,

$$\ker(f) = \{\overline{x} \in A/I \mid \widehat{x} = \widehat{0}\} = \{\overline{x} \in A/I \mid x \in J\} = J/I.$$

et

$$\mathrm{Im}(f) = A/J.$$

D'après le premier théorème d'isomorphisme, on a le résultat. □

1.7 Iéaux premiers et idéaux maximaux

Définition 1.12.1. Un idéal P d'un anneau A est dit premier si $P \neq A$ et pour tous $x, y \in A$, on a $xy \in P$ implique $x \in P$ ou $y \in P$.

***Exemples* 1.12.1.**
1. $\{0\}$ est idéal premier de $\mathbb{Z}$.
2. Les idéaux premiers de $\mathbb{Z}$ sont $\{0\}$ et $p\mathbb{Z}$ avec p un entier premier.

Proposition 1.13

Un anneau A est intègre si et seulement si $\{0\}$ est un idéal premier de A.

Démonstration. Découle des définitions des idéaux premiers et des anneaux intègres. □

Scanned with CamScanner

Proposition 1.14

Un idéal P d'un anneau A est premier si et seulement si A/P est intègre.

Démonstration. Supposons que P est premier. Soient $x, y \in A$ tels que $\overline{xy} = \overline{x}.\overline{y} = \overline{0}$. Donc, $xy \in P$. Ainsi, $x \in P$ ou $y \in P$. Par suite, $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Par conséquent, A/P est intègre.
Supposons que A/P est intègre. Soient $x, y \in A$ tels que $xy \in P$. Donc, $\overline{x}.\overline{y} = \overline{xy} = \overline{0}$. Comme A/P est intègre, $\overline{x} = \overline{0}$ ou $\overline{y} = \overline{0}$. Donc, $x \in P$ ou $y \in P$, et ainsi P est premier. □

Définition 1.14.1. Soit A un anneau. Un idéal I est dit maximal s'il est propre ($I \neq A$) et si les seuls idéaux de A contenant I sont I et A.

Théoreme 1.15 (Admis)

1. Tout anneau non nul possède au moins un idéal maximal.
2. Dans un anneau non nul, tout idéal propre est contenu dans un idéal maximal.

Proposition 1.16

Un idéal M d'un anneau A est maximal si et seulement si l'anneau A/M est un corps.

Démonstration. Supposons que M est maximal. Soit $x \in A$ tel que $\overline{x} \neq \overline{0}$. Donc, $x \notin M$. Par suite, $M \subsetneq M + (x)$. Ainsi, $M + (x) = A$. Alors, il existe $m \in M$ et $a \in A$ tels que $m + ax = 1$. D'où, $\overline{ax} = \overline{1}$. Ainsi, $\overline{x}$ est inversible te A/M est un corps.
Supposons que A/M est un corps. Soit I un ideal de A tel que $M \subseteq I$. Donc, I/M est un idéal de A/M qu'est un corps. Alors, $I/M = \{\overline{0}\}$ ou $I/M = A/M$. Alors, $I = M$ ou $I = A$. Par conséquent, M est maximal. □

Proposition 1.17

Tout idéal maximal est premier.

Démonstration. Soit M un idéal maximal d'un anneau A. Alors, A/M est un corps, et donc intègre. Par suite, M est premier. □

Remarque 1.17.1. La réciproque n'est pas vraie en général. Dans l'anneau $\mathbb{Z}$, l'idéal $\{0\}$ est premier puisque $\mathbb{Z}$ est intègre mais non maximal puisque $\mathbb{Z}$ n'est pas un corps.

Scanned with CamScanner

Proposition 1.18

Soient A un anneau et I un idéal de A. Les idéaux premiers (resp. maximaux) de A/I sont les idéaux de la forme P/I avec P un idéal premier (resp. maximal) de A contenant I.

Démonstration. Exercice. □

Scanned with CamScanner

Chapitre 2

Anneaux euclidiens, principaux, factoriels

Dans tout le chapitre, les anneaux considérés sont commutatifs.

2.1 Anneaux euclidiens et principaux

On peut faire des divisions euclidiennes dans les anneaux $\mathbb{Z}$ et $\mathbb{K}[X]$ où $\mathbb{K}$ est un corps. Ici, Nous allons généraliser cette situation.

Définition 2.18.1. Soient A un anneau et $a, b \in A$. On dit que a divise b, et on note a/b, s'il existe $c \in A$ tel que $b = ac$.

Définition 2.18.2 (Anneau euclidien)**.** Un anneau intègre A muni d'une application $\nu : A^* \to \mathbb{N}$, appelée stathme ou mesure, telle que :

1. pour tous $a, b \in A^*$, a/b implique $\nu(a) \leq \nu(b)$, et
2. pour tous $a, b \in A$ avec b non nul, il existe des éléments $q, r \in A$ tels que $a = bq+r$ avec $r = 0$ ou $\nu(r) < \nu(b)$,

est dit anneau euclidien.

***Exemples* 2.18.1.**

1. $\mathbb{Z}$ est un anneau euclidien pour le stathme $\nu : \mathbb{Z}^* \to \mathbb{N}$; $\nu(n) = |n|$.
2. $\mathbb{R}[X]$ est un anneau euclidien pour le stathme $\nu : \mathbb{R}[X]^* \to \mathbb{N}$; $\nu(P) = \deg(P)$.
3. $\mathbb{Z}\left[i\sqrt{2}\right]$ est un anneau euclidien pour le stathme $\nu : \mathbb{Z}\left[i\sqrt{2}\right]^* \to \mathbb{N}$; $\nu(z) = |z|^2$.
4. $\mathbb{Z}[i]$ est un anneau euclidien pour le stathme $\nu : \mathbb{Z}[i]^* \to \mathbb{N}$; $\nu(z) = |z|^2$.

Remarque 2.18.1. Dans la définition d'un anneau euclidien, on ne demande pas l'unicité de la division avec reste. En effet, même dans $\mathbb{Z}$, cette division n'est pas unique. Par exemple, si l'on prend $a = 8$ et $b = 3$, $8 = 3.2 + 2$ et $8 = 3.3 + (-1)$ sont deux divisions avec reste possibles.

Scanned with CamScanner

Définition 2.18.3. Un anneau intègre est dit principal si tout idéal de A est principal ; c'est à dire que pour tout idéal I de A il existe $x \in A$ tel que $I = Ax = \{ax \mid a \in A\}$.

***Exemples* 2.18.2.**

1. Les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ avec n un entier positif ou nul, l'anneau $\mathbb{Z}$ est donc principal.
2. Les idéaux de l'anneau $\mathbb{Z}_4$ sont le $\{\overline{0}\}$, $2\mathbb{Z}_4$ et $\mathbb{Z}_4$. Donc, tout idéal de $\mathbb{Z}_4$ est principal. Cependant, l'anneau $\mathbb{Z}_4$ n'est pas intègre, et donc l'anneau n'est pas principal.
3. L'anneau $\mathbb{Z}[X]$ est intègre mais pas principal. Pour voir cela, on pose $I =< 2, X >= 2\mathbb{Z}[X] + X\mathbb{Z}[X]$. On suppose que $I =< P >$ avec $P \in \mathbb{Z}[X]$. Donc, $2 = PQ$ pour un certain $Q \in \mathbb{Z}[X]$. Cela implique que P et Q sont des polynômes consatnts dans $\mathbb{Z}[X]$, et $P = \pm 1$ ou $P = \pm 2$. De même, $X = PS$ avec $S \in \mathbb{Z}[X]$, ce qui implique que $S = \alpha X$ avec $\alpha \in \mathbb{Z}$. Donc, $1 = P\alpha$. Ainsi, P est inversible dans $\mathbb{Z}$. Alors, $P = \pm 1$. Donc, $1 \in I$, et cela entaîne l'existance de $T, R \in \mathbb{Z}[X]$ tels que $1 = 2T + XR$. Ainsi, $1 = 2T(0)$, ce qu'est impossible.

Théoreme 2.19

Tout anneau euclidien est principal.

Démonstration. Soit A un anneau euclidien pour le stathme ν, et soit $(0) \subsetneq I \subsetneq A$ un idéal de A. On considère l'ensemble $F = \{\nu(x) \mid x \in I\}$. L'ensemble $F \subseteq \mathbb{N}$ est non vide, et donc admet un plus petit élément a. Soit $x \in I$. Il existe $q, r \in A$ tels que $x = aq + r$ avec $r = 0$ ou $\nu(r) < \nu(a)$. En plus, $r = x - aq \in I$, et donc, si $r \neq 0$, on a $\nu(r) \geq \nu(a)$, ce qu'est impossible car $\nu(r) < \nu(a)$. Ainsi, $r = 0$, et par suite, $x \in Aa$. Par conséquent, $I \subseteq Aa \subseteq I$. D'où, I est principal. □

Remarque 2.19.1.

1. La réciproque du théorème précédent est fausse. En effet, l'anneau $\mathbb{Z}\left[\frac{1 + \sqrt{19}i}{2}\right]$ est prinical mais pas euclidien.
2. A principal $\not\Longrightarrow A[X]$ principal et A euclidien $\not\Longrightarrow A[X]$ euclidien. Un simple contre-exemple est donné par l'anneau $\mathbb{Z}$ qu'est euclidien (et donc principal) mais $\mathbb{Z}[X]$ n'est pas principal (et donc n'est pas euclidien).

Lemme 2.20

Dans un anneau principal, tout idéal premier non nul est maximal

Démonstration. Soit A un anneau principal et $I = Ax$ un idéal premier. On suppose que $I \subseteq J = Ay$. Dans, $x = ay$ avec $a \in A$. Comme I est premier, on a $a \in I$ ou $y \in I$. Si

Scanned with CamScanner

$y \in I$, alors $J = Ay \subseteq I$. D'où, $I = J$. Si maintenant $a \in I$, alors $a = bx$ avec $b \in A$. Donc, $x = xby$, ce qui implique que $1 = by$ (car A est intègre), et donc y est inversible. Par suite $J = A$. D'où, I est maximal. □

Théoreme 2.21

Soit A un anneau. Alors,

$$A[X] \text{ euclidien } \Leftrightarrow A[X] \text{ principal } \Leftrightarrow A \text{ corps.}$$

Démonstration. Il suffit de montrer que si $A[X]$ est principal alors A est un corps. Les autres implications sont claires.
L'application

$$\begin{array}{rccc} f: & A[X] & \longrightarrow & A \\ & P & \longmapsto & P(0) \end{array}$$

est un morphisme d'anneaux surjectif, et $\ker(f) = \{P \in A[X] \mid P(0) = 0\} = XA[X]$. En utilisant le premier théorème d'isomorphisme, on obtient $A \cong A[X]/ < X >$. Comme $A[X]$ est principal, il est intègre. Donc, A l'est aussi. Ainsi, $< X >$ est premier dans $A[X]$ et donc maximal. Par conséquent, A est un corps. □

2.2 Divisibilité

Soient A un anneau et a, b deux éléments de A. Rappelons que a divise b, noté a/b, s'il existe $c \in A$ tel que $b = ac$. Les diviseurs de 1 sont les unités de l'anneau ; ce sont les éléments inversibles pour la multiplication. Ils forment un groupe noté $U(A)$.

Définition 2.21.1. Soient A un anneau et a, b deux éléments de A. On dit que a est associé à b, s'il existe une unité u de A tel que $a = ub$. Il est facile de voir qu'« être associé » est une relation d'équivalence sur A.

Définition 2.21.2. Soit A un anneau.

1. Un élément p de A est premier si $p \neq 0$ et $< p >$ est un idéal premier de A. De façon équivalente, p est premier si et seulement si $p \neq 0$, p n'est pas une unité et pour tous $a, b \in A$ si p/ab, alors p/a ou p/b.
2. Un élément q de A est irréductible si $q \neq 0$, q n'est pas une unité de A et si pour tous $a, b \in A$ tels que $q = ab$, on a $a \in U(A)$ ou $b \in U(A)$.

Scanned with CamScanner

Remarque 2.21.1. Un élément associé à un élément premier (resp. irréductible) est aussi premier (resp. irréductible).

Proposition 2.22

Soient A un anneau intègre et q un élément de A. Alors, q est irréductible si et seulement si $< q >$ est un idéal maximal dans l'ensemble des idéaux principaux de A différent de A.

Démonstration. Supposons que q est irréductible. Soit $x \in A$ tel que $< q > \subseteq < x > \subsetneq A$. Montrons que $< q > = < x >$ (c'est à dire que x et q sont associés). Le fait que $< x > \subsetneq A$ veut dire que $x \notin U(A)$. Aussi, $q \in < x >$ et donc il existe $y \in A$ tel que $q = xy$. Comme q est irréductible, on déduit que $y \in U(A)$, et donc x et y sont associés.
Inversement, supposons que $< q >$ est un idéal maximal dans l'ensemble des idéaux principaux de A différent de A. Posons $q = xy$ avec $x, y \in A$ et $x \notin U(A)$. On a $< q > \subseteq < x > \subsetneq A$, et donc $< q > = < x >$. Par suite, q et x sont associés. Alors, il existe $u \in U(A)$ tel que $q = ux$. Comme A est intègre et $x \neq 0$, on déduit que $y = u$. □

Proposition 2.23

Soit A un anneau intègre. Tout élément premier de A est irréductible.

Démonstration. Soit p un élément premier de A. Alors, $p \neq 0$ et p n'est pas une unité. Soient $a, b \in A$ tels que $p = ab$. Donc, p/a ou p/b. Si par exemple p/a, alors $a = ps$ avec $s \in A$. Donc, $p = psb$. Par intègrité de A, on obtient $1 = sb$, et donc $b \in U(A)$. De même, si p/b on obtient $a \in U(A)$ Par suite, p est irréductible. □

La réciproque de cette proposition est vraie pour certains anneaux mais ce n'est pas toujours le cas.

***Exemple* 2.23.1.** Dans $A = \mathbb{Z}\left[\sqrt{5}i\right]$ l'élément 2 est irréductible mais pas premier.

Démonstration.
— Montrons que 2 est irréductible. Supposons que $2 = z_1 z_2$ avec $z_1, z_2 \in A$. On a $4 = |z_1 z_2|^2 = |z_1|^2 |z_2|^2$. Or, $|z_1|^2, |z_2|^2 \in \mathbb{N}$. Donc, $|z_1|^2 = 1, 2 ou 4$. On pose $z_1 = a + b\sqrt{5}i$ avec $a, b \in \mathbb{Z}$. Donc, $|z_1|^2 = a^2 + 5b^2$. Si $|z_1|^2 = 1$ alors $z = \pm 1$, et donc $z_1 \in U(A)$. De même, si $|z_1|^2 = 4$ alors $|z_2|^2 = 1$ et donc $z_2 \in U(A)$. Le dérnier cas $|z_1|^2 = a^2 + 5b^2 = 2$ est impossible.
— Montrons que 2 n'est pas premier. On a $6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$. Si 2 était un élément premier, il diviserait $1 + \sqrt{5}i$ ou $1 - \sqrt{5}i$. Considérons par exemple le premier cas. Il existe un élément z de A tel que $1 + \sqrt{5}i = 2z$. Donc, $6 = |1 + \sqrt{5}i|^2 = 4|z|^2$, ce qui est impossible.

Scanned with CamScanner

□

Proposition 2.24

Soient A un anneau principal. Alors, tout élément irréductible de A est premier.

Démonstration. Soit q un élément irréductible de A. On sait que $< q >$ est un idéal maximal dans l'ensemble des idéaux principaux de A (différent de A). Mais comme A est principal, tout idéal est principal, et donc $< q >$ est un idéal maximal. Par suite, $< q >$ est un idéal premier, et donc q est premier. □

Définition 2.24.1. Soit A un anneau intègre. Deux éléments a et b de A sont dits premiers entre eux si les seuls diviseurs en commun sont les unités de A.

Proposition 2.25

Soit A un anneau intègre. Alors, tout élément irréductible est premier avec tout élément qu'il ne divise pas.

Démonstration. Soit q un élément irréductible de A et soit $a \in A$ tel que q ne divise pas a. Soit aussi d un diviseur en commun de q et x. Donc, $d \in U(A)$ ou d est associé à q. Dans le second cas, $x \in < d >=< q >$, et donc q divise x, ce qu'est absurde. Donc, $d \in U(A)$, et q et x sont premiers entre eux. □

Définition 2.25.1. Soient A un anneau intègre et a et b deux éléments de A. On dit que a et b admettent un plus grand commun diviseur (pgcd) si :

1. il existe $d \in A$ tel que d divise a et b, et
2. si $d' \in A$ divise a et b alors d' divise d.

Remarque 2.25.1. Soient A un anneau intègre et a et b deux éléments de A.

1. Si a divise b alors a est un pgcd de a et b.
2. Il existe des anneaux dans lesquels le pgcd de deux éléments n'existe pas toujours. Notamment, dans l'anneau $A = \mathbb{Z}\left[\sqrt{5}i\right]$ les éléments $z_1 = 2(1 + \sqrt{5}i)$ et $z_2 = 6 = (1 + \sqrt{5}i)(1 - \sqrt{5}i)$ n'ont pas de pgcd. En effet, supposons que d soit un pgcd de ces deux éléments. Comme d divise z_1 et z_2, sa norme $|d|^2$ divise $|z_1|^2 = 24$ et $|z_2|^2 = 36$. D'autre part comme 2 et $(1 + \sqrt{5}i)$ sont des diviseurs communs, $|d|^2$ est divisible par 4 et 6. On en déduit facilement que $|d|^2 = 12$. Ceci est impossible car l'équation $a^2 + 5b^2 = 12$ n'a pas de solution dans $\mathbb{Z}$.

Scanned with CamScanner

Proposition 2.26

Soient A un anneau intègre et a et b deux éléments de A admettant un pgcd d. Alors, $d' \in A$ est un pgcd de a et b si et seulement si d' est associé à d.

Démonstration. ($\Rightarrow$) Par définition de pgcd, d divise d' et d' divise d. Donc, d et d' sont associés.
($\Leftarrow$) On pose $d' = ud$ avec $u \in U(A)$. On a $d \in A$ tel que d divise a et b, et donc d' divise a et b. Soit d" $\in A$ tel que d" divise a et b. Donc, d" divise d, et par suite d" divise d'. Par conséquent, d' est un pgcd de a et b. □

2.3 Anneaux factoriels

Définition 2.26.1 (Décomposition unique en produit de facteurs irréductibles)**.** Soit A un anneau intègre. On dit qu'un élément non nul a de A admet une décomposition unique en produit de facteurs irréductibles si les deux conditions suivantes sont satisfaites.

1. Il existe une unité $u \in A$, un entier $r \geq 1$, des éléments irréductibles $p_1, \cdots, p_r$ de A, des entiers $k_1, ..., k_r \geq 1$ tels que
$$a = up_1^{k_1} \cdots p_r^{k_r}.$$
2. Si a admet une seconde décomposition du même type : $a = vq_1^{l_1} \cdots q_s^{l_s}$, alors $r = s$ et il existe une permutation σ des indices telle qu'on ait $p_{\sigma(i)}$ associé à q_i et $k_{\sigma(i)} = l_i$ pour $i = 1, ..., r$.

Il est souvent utile de normaliser la décomposition en facteurs irréductibles. Pour cela, on choisit une famille $(p_i)_{i\in I}$ d'éléments irréductibles de A telle que :

1. tout élément irréductible de A est associé à l'un des p_i,
2. si $i \neq j$, p_i et p_j ne sont pas associés.

Ce choix étant effectué, la définition précédente s'énonce : a s'écrit de manière unique sous la forme
$$a = u \prod_{i\in I} p_i^{r_i}.$$
où u est un élément inversible de A et où les r_i sont des entiers positifs, nuls sauf un nombre fini d'entre eux.

Définition 2.26.2 (Anneau factoriel)**.** Un anneau A est dit factoriel s'il est intègre et si tout élément non nul admet une décomposition unique en produit de facteurs irréductibles.

Scanned with CamScanner

Dans un anneau factoriel, un élément $a = u\prod_{i\in I} p_i^{r_i}$ divise donc un élément $b = v\prod_{i\in I} p_i^{s_i}$ si et seulement si pour tout i on a $r_i \leq s_i$. En effet, si $c \in A$ tel que $b = ac$, on écrit $c = w\prod_{i\in I} p_i^{t_i}$ puis on observe que l'on a $v\prod_{i\in I} p_i^{s_i} = uw\prod_{i\in I} p_i^{r_i+t_i}$. D'où, par unicité, que $s_i = r_i + t_i$ pour tout i. Inversement, il suffit de prendre $c = u^{-1}v\prod_{i\in I} p_i^{s_i-r_i}$.

Lemme 2.27

Dans un anneau factoriel, tout élément irréductible est premier.

Démonstration. On va montrer que si a est irréductible et si a/bc alors a/b ou a/c. Pour simplifier on va supposer avoir normalisé la décomposition en facteurs irréductibles dans A. Comme a est irréductible, on a $a = up_j$ pour un $j \in I$. On pose aussi $b = v\prod_{i\in I} p_i^{s_i}$ et $c = w\prod_{i\in I} p_i^{t_i}$ les décompositions en facteurs irréductibles de b et c. Comme a divise bc, on sait que $s_j + t_j \geq 1$. Mais alors $s_j \geq 1$ ou $t_j \geq 1$. En particulier, a divise b ou c. □

Proposition 2.28

Soit A un anneau factoriel et $a = u\prod_{i\in I} p_i^{r_i}$ et $b = v\prod_{i\in I} p_i^{s_i}$ deux élément de A, alors $d = \prod_{i\in I} p_i^{\inf\{r_i,s_i\}}$ est un pgcd de a et b.

Démonstration. Il est clair que d divise a et b. Si $d' = w\prod_{i\in I} p_i^{t_i}$ divise a et b alors, $t_i \leq \inf\{r_i, s_i\}$, et donc d' divise d. □

Lemme 2.29

Dans un anneau principal, toute suite croissante d'idéaux est stationnaire.

Démonstration. Supposons par l'absurde qu'il existe une suite $(a_1) \subset (a_2) \subset \cdots$ une suite strictement croissante d'idéaux. On pose $J = \bigcup_{i\geq 1}(a_i)$. Montrons que J est un idéal. Il est clairement non vide. Si $x, y \in J$ alors il existe $i, j \geq 1$ tel que $x \in (a_i)$ et $y \in (a_j)$. Si par exemple $i \leq j$ alors $x \in (a_i) \subset (a_j)$ et donc $x - y \in (a_j) \subset J$. En plus, pour tout $a \in A$, $ax \in (a_i) \subset J$. Par suite, J est un ideal de A, et donc principal. On pose $J = (a)$. Alors, il existe $i \geq 1$ tel que $a \in (a_i)$, et donc pour tout $j \geq i$, $J \subset (a_i) \subset (a_j) \subset (a_j) \subset J$. Par conséquent, $(a_i) = (a_j)$ ce qu'est absurde. □

Scanned with CamScanner

Lemme 2.30

Soit A un anneau principal et $a \in A$ non nul et non inversible. Alors il existe $n \geq 0$, des éléments irréductibles $p_1, \cdots, p_n$ de A et un inversible u de A tels que $a = up_1 \cdots p_n$.

Démonstration. Supposons par l'absurde qu'il existe un élément a non nul de A qui n'est pas produit d'éléments irréductibles. Soit $a_1 = a$. L'élément a n'est pas inversible (sinon $a = u$ avec u inversible serait une décomposition), ni irréductible (sinon $a = p$ avec p irréductible serait une décomposition). Soit $a = bc$ avec b et c non inversibles. Comme a n'est pas produit fini d'éléments irréductibles, b ou c n'est pas produit fini d'éléments irréductibles. Soit a_2 cet élément. L'idéal (a_2) contient donc strictement l'idéal (a_1). On construit ainsi, par récurrence, une suite $a_1, a_2, \cdots$ d'éléments de A tels que la suite d'idéaux $(a_1) \subset (a2) \subset \cdots$. soit strictement croissante, ce qu'est impossible. Tout élément non nul d'un anneau principal admet donc une décomposition en éléments irréductibles. □

Théoreme 2.31

Tout anneau principal est factoriel.

Démonstration. Soit $a \in A$ non nul. L'existence de la décomposition de a en éléments irréductibles est assurée par le lemme précédent. Donc, il suffit de proouver l'unicité. Supposons que $a = up_1^{k_1} \cdots p_r^{k_r} = vp_1^{l_1} \cdots p_r^{l_r}$ avec des k_i et l_i pas tous égaux. Effectuons toutes les simplifications possibles. S'il reste dans le membre de gauche un facteur p irréductible, il divise le produit de facteurs irréductibles de droite, et comme il est premier, il en divise l'un des termes qui est donc associé à p, contrairement aux simplifications effectuées. Il ne peut donc rester aucun facteur irréductible dans l'un des membres, ce qui montre l'unicité. □

2.4 Théorème de Gauss : Si l'anneau A est factoriel alors l'anneau $A[X]$ est factoriel

Définition 2.31.1. Soit A un anneau factoriel et soit $P \in A[X]$. Le contenu de P, noté $c(P)$, est un pgcd des coefficients de P. On dira que P est primitif si $c(P)$ est inversible.

Scanned with CamScanner

Proposition 2.32

Soit A un anneau factoriel et soient $P, Q \in A[X]$. Alors, $c(PQ) \sim c(P)c(Q)$.

Démonstration. Soient P et Q des polynômes primitifs. Supposons que PQ ne soit pas un polynôme primitif, autrement dit que $c(PQ)$ soit non inversible dans A. Soit $p \in A$ un facteur irréductible de $c(PQ)$. L'idéal $I = pA$ est un idéal premier et l'anneau A/I est intègre. Notons $\pi : A[X] \to (A/I)[X]$ l'homomorphisme de changement d'anneau induit par la projection canonique $A \to A/I$. Comme $\pi(PQ) = \pi(P)\pi(Q)$ est nul, $\pi(P)$ ou $\pi(Q)$ est nul, donc P ou Q est divisible par p. Le contenu de l'un des deux polynômes, divisible par p, n'est pas inversible, ce qui donne une contradiction et montre que PQ est un polynôme primitif.
Supposons maintenant que P et Q ne sont pas primitif, et posons $P = c(P)P'$ et $Q = c(Q)Q'$ avec P' et Q' sont primitifs. Donc, $c(PQ) = c(P)c(Q)c(P'Q') \sim c(P)c(Q)$. □

Proposition 2.33

Soit A un anneau factoriel et K son corps de fractions. Alors les éléments irréductibles de $A[X]$ sont exactement :

- les éléments irréductibles de A ;
- les polynômes primitifs de $A[X]$, irréductibles en tant que polynômes de $K[X]$.

Démonstration. Montrons d'abord que les éléments en question sont bien irréductibles. Soit donc $a \in A$ irréductible et supposons que $P, Q \in A[X]$ sont tels que $a = PQ$. Comme A est intègre, on a $\deg(P) + \deg(Q) = \deg(PQ) = 0$, donc P et Q sont nécessairement de degré 0, ou autrement dit des éléments de A. L'élément a étant irréductible dans A, la relation est banale dans A et donc aussi dans $A[X]$. L'élément a est donc bien irréductible dans l'anneau $A[X]$.
Soit maintenant $P \in A[X]$ primitif, irréductible dans $K[X]$ et supposons $P = QR$ avec Q et R dans $A[X]$. Vu dans $K[X]$ cette relation doit être banale ou autrement dit, Q ou R est inversible dans $K[X]$, c'est-à-dire constant. Supposons que cela soit Q. Nous avons $c(P) = c(Q)c(R) = Qc(R)$, puisque Q est constant. Comme P est primitif, $c(P) \sim 1$ et l'élément Q est nécessairement inversible dans A donc dans $A[X]$. Ainsi, P est irréductible dans $A[X]$.
Montrons maintenant que les éléments en question sont les seuls éléments irréductibles. Pour cela, soit P un élément irréductible de $A[X]$ et écrivons $P = c(P)P'$ avec P' primitif. Cette relation doit être banale, donc $c(P) \sim 1$ ou P' est inversible dans $A[X]$. On va montrer que dans le premier cas, P est irréductible dans $K[X]$ et que dans le second cas $c(P)$ est irréductible.

Scanned with CamScanner

Dans le premier cas, P est primitif. Soit $P = QR$ une factorisation avec $Q, R \in K[X]$. On peut écrire $Q = qQ'$ et $R = rR'$, où q et r sont dans K et où Q' et R' sont deux polynômes primitifs de $A[X]$. En effet, on sort d'abord le dénominateur commun des coefficients, puis on sort le contenu. On a ainsi $P = (qr)Q'R'$. La fraction qr s'écrit $\frac{a}{b}$ où $a, b \in A$. On obtient $bP = aQ'R'$ dans $A[X]$. Ces deux polynômes ont donc le même contenu, a et b respectivement. Par conséquent, $a \sim b$, d'où $qr = u \in U(A)$, ce qui donne la relation $P = uQ'R'$ dans $A[X]$. Comme P est irréductible dans $A[X]$, $Q' \in U(A)$ ou $Q' \in U(A)$. D'où, $Q \in K$ ou $R \in K$.
Dans le second cas, P' est constant, inversible dans A. On observe alors qu'une relation non banale $c(P) = ab$ dans A nous donnerait une relation non banale $P = a(bP')$ dans $A[X]$, ce qui contredit l'hypothèse que P est irréductible. □

Comme on voit dans la proposition ci-dessus, le corps de fraction K de l'anneau factoriel A joue un rôle important dans la description des éléments irréductibles de $A[X]$. Comme K est un corps, l'anneau $K[X]$ est principal et donc en particulier factoriel d'après le théorème. On va utiliser cette observation pour démontrer le théorème de Gauss.

Démonstration du théorème de Gauss. Notons K le corps de fraction de A. Il faut montrer que tout polynôme P de $A[X]$ admet une décomposition unique en produit de facteurs irréductibles. Nous allons montrer l'existence de la décomposition au (1) et (2), l'unicité au (4) à l'aide d'un lemme donné au (3).

1. Supposons P primitif. Comme $K[X]$ est euclidien, donc factoriel, il existe une décomposition de P en produit de facteurs irréductibles dans $K[X]$: $P = \prod_{i=1}^{r} P_i$. En réduisant les coefficients de chacun des P_i au même dénomidinateur, on peut écrire $Pi = \frac{a_i}{b_i} Q_i$, avec Q_i primitif et irréductible dans $A[X]$. On a $\left(\prod_{i=1}^{r} b_i\right) P = \prod_{i=1}^{r} a_i Q_i$, d'où, en simplifiant par les contenus des deux membres, $P = v \prod_{i=1}^{r} Q_i$ où v est une unité de A ; ceci montre l'existence d'une décomposition de P dans $A[X]$ en produit de facteurs irréductibles dans le cas où P primitif.
2. Si P n'est primitif, écrit $P = c(P)P_1$ et décompose $c(P)$ dans A et P_1 comme précédemment pour obtenir une décomposition de P.
3. Montrons qu'un élément irréductible F de $A[X]$ est premier dans $A[X]$. Si F est un élément irréductible p de A (et donc premier dans A), on a $\frac{A[X]}{pA[X]} \cong \frac{A}{pA}[X]$. Comme ce dernier anneau est intègre, p est premier dans $A[X]$. Si F n'est pas dans A, on a vu que $c(F) \sim 1$ et que F est irréductible dans $K[X]$. Si F divise dans $A[X]$ un produit GH de deux polynômes de $A[X]$, F divise GH dans $K[X]$; comme $K[X]$

Scanned with CamScanner

est factoriel, F divise G, par exemple, et il existe un polynôme G' de $K[X]$ tel que $FG' = G$. Écrivons $G' = (a/b)G_1$ avec G_1 dans $A[X]$ primitif et $a, b \in A$ premiers entre eux. On a alors $bG = bFG' = aFG_1$. En prenant le contenu de chaque côté, on voit $bc(G) = a$ d'où $a/b = c(G) \in A$. On a donc $G' \in A[X]$, ce qui montre que F divise Q dans A[X].

4. 4) Supposons que P admet deux décompositions en produit de facteurs irréductibles dans $A[X]$: $P = u\prod_{i=1}^{r} P_i = u\prod_{j=1}^{s} T_j$. Après avoir simplifié par les facteurs associés des deux membres, s'il reste un facteur P_i, il est premier d'après (3), donc divise un des facteurs de droite T_j ; ces deux facteurs sont associés, contradiction et fin de la démonstration.

□

Scanned with CamScanner

Série 1

Anneaux et idéaux.

Exercice 1. On définit sur $\mathbb{Z}^2$ deux lois de composition internes notées $+$ et $*$ et définies, pour tous $(a,b),(c,d) \in \mathbb{Z}^2$, par :

$$(a,b)+(c,d)=(a+c,b+d) \text{ et } (a,b)*(c,d)=(ac+2bd,ad+bc).$$

(1) Montrer que $(\mathbb{Z}^2,+,*)$ est un anneau commutatif.

(2) Montrer que $\mathbb{Z}\times\mathbb{Z} \cong \mathbb{Z}[\sqrt{2}]$.

Exercice 2. Soit $A=\left\{\frac{m}{n} \mid m\in\mathbb{Z},\ n\in 2\mathbb{Z}+1\right\}$ (c'est-à-dire que A est l'ensemble des rationnels à dénominateur impair).

(1) Démontrer que A est un sous anneau de $(\mathbb{Q},+,\times)$.

(2) Quels sont ses éléments inversibles ?

Exercice 3. On considère $\mathbb{Z}\left[\sqrt{2}\right]=\left\{a+b\sqrt{2} \mid a,b\in\mathbb{Z}\right\}$.

(1) Montrer que $\left(\mathbb{Z}\left[\sqrt{2}\right],+,\times\right)$ est un anneau.

(2) On note $N\left(a+b\sqrt{2}\right)=a^2-2b^2$. Montrer que, pour tous x et y de $\mathbb{Z}\left[\sqrt{2}\right]$, on a $N(xy)=N(x)N(y)$.

(3) En déduire que les éléments inversibles de $\mathbb{Z}\left[\sqrt{2}\right]$ sont ceux s'écrivant $a+b\sqrt{2}$ avec $a^2-2b^2=1$.

Exercice 4 (Anneau de Boole)**.** On dit qu'un anneau A non réduit à $\{0\}$ est un anneau de Boole si, pour tout $x\in A$, on a $x^2=x$. On fixe A un tel anneau.

(1) Montrer que $(\forall x,y\in A)$, on a $xy+yx=0$. En déduire que, pour tout $x\in A$, on a $x=-x$.

(2) Montrer que A est commutatif.

(3) Montrer que $(\forall x,y\in A)$, on a $xy(x+y)=0$. En déduire qu'un anneau de Boole intègre ne peut avoir que deux éléments.

Exercice 5. Pour tout $a\in\mathbb{R}$, on pose $I_a=\{P\in\mathbb{R}[X] \mid P(a)=0\}$.

(1) Montrer que I_a est un ideal de $\mathbb{R}[X]$.

(2) Montrer que si $a\neq b$, alors $I_a+I_b=\mathbb{R}[X]$.

Exercice 6. Soit A un anneau et e un idempotent (c-à-d, $e^2=e$).

(1) Montrer que $1-e$ est encore idempotent.

(2) Montrer que eA et $(1-e)A$ sont des idéaux étrangers dans A.

(3) En déduire que $A\cong A/eA\times A/(1-e)A$.

Scanned with CamScanner

Exercice 7. On considère l'anneau $\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}$. On note $(2, X) := 2\mathbb{Z}[X] + X\mathbb{Z}[X]$ l'idéal de $\mathbb{Z}[X]$ engendré par 2 et X.

(1) Montrer que $(2, X)$ n'est pas principal.

(2) Montrer que l'application $f : \mathbb{Z}[X] \to \mathbb{Z}/2\mathbb{Z}$ définie par $f(P) = \overline{P(0)}$ est un morphisme d'anneaux surjectif.

(3) Montrer que $\ker(f) = (2, X)$.

(4) En déduire que $\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}$

(5) Que peut-on dire de l'idéal $(2, X)$?

Exercice 8 (Idéaux premiers)**.**

(1) Montrer que les idéaux premiers non nuls de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ avec p un entier premier.

(2) Soit $P \in \mathbb{R}[X]$ un polynôme irréductible. Montrer que $P\mathbb{R}[X] = \{PQ \mid Q \in \mathbb{R}[X]\}$ est idéal premier de $\mathbb{R}[X]$.

(3) Soit A un anneau commutatif dont tout idéal est premier. Etablir que A est intègre puis que A est un corps.

Exercice 9. Soient A et B deux anneaux commutatifs.

(1) Montrer que les idéaux de $A \times B$ sont exactemenet les ensembles $I \times J$ avec I un idéal de A et J un idéal de B.

(2) Montrer qu'un idéal premier de $A \times B$ est de la forme $P \times B$ avec P un idéal premier de A ou de la forme $A \times Q$ ou Q est un ideal premier de B.

(3) Montrer qu'un idéal maximal de $A \times B$ est de la forme $P \times B$ avec P un idéal maximal de A ou de la forme $A \times Q$ ou Q est un ideal maximal de B.

(4) On suppose que A et B sont des corps. Donner tous les idéaux maximaux de $A \times B$.

Exercice 10. Soit A un anneau commutatif unitaire.

(1) On suppose que A n'admet que les idéaux triviaux $\{0\}$ et A. Démontrer que A est un corps.

(2) On suppose que A est intègre et qu'il n'admet qu'un nombre fini d'idéaux. Démontrer que A est un corps.

(3) En déduire que tout anneau commutatif unitaire intègre fini est un corps.

Scanned with CamScanner

Série 1

Anneaux et idéaux.

Exercice 1. On définit sur $\mathbb{Z}^2$ deux lois de composition internes notées $+$ et $*$ et définies, pour tous $(a,b),(c,d) \in \mathbb{Z}^2$, par :

$$(a,b)+(c,d) = (a+c, b+d) \text{ et } (a,b)*(c,d) = (ac+2bd, ad+bc).$$

(1) Montrer que $(\mathbb{Z}^2, +, *)$ est un anneau commutatif unitaire.

(2) Montrer que $\mathbb{Z}\times\mathbb{Z} \cong \mathbb{Z}[\sqrt{2}]$.

Solution.

(1) Montrons que $(\mathbb{Z}^2, +, *)$ est un anneau commutatif unitaire :

— On sait que $(\mathbb{Z}^2, +)$ est un group abélien.
— Pour tout $(a,b) \in\in \mathbb{Z}^2$, on $(a,b)*(1,0) = (a,b)$.
— Pour tous $(a,b),(c,d) \in \mathbb{Z}^2$, on a

$$(a,b)*(c,d) = (ac+2bd, ad+bc) = (ca+2db, cb+da) = (c,d)*(a,b).$$

Donc, $*$ est commutative.
— Pour tous $(a_1,a_2),(b_1,b_2),(c_1,c_2) \in \mathbb{Z}^2$, on a

$$\begin{aligned}
(a_1,a_2)*\Big((b_1,b_2)*(c_1,c_2)\Big) &= (a_1,a_2)*(b_1c_1+2b_2c_2, b_1c_2+b_2c_1)\\
&= \Big(a_1(b_1c_1+2b_2c_2)+2a_2(b_1c_2+b_2c_1), a_1(b_1c_2+b_2c_1)+a_2(b_1c_1+2b_2c_2)\Big)\\
&= \Big((a_1b_1+2a_2b_2)c_1+2(a_1b_2+a_2b_1)c_2+, (a_1b_1+2a_2b_2)c_2+(a_1b_2+a_2b_1)c_1)\Big)\\
&= (a_1b_1+2a_2b_2, a_1b_2+a_2b_1)*(c_1,c_2)\\
&= \Big((a_1,a_2)(*(b_1,b_2)\Big)*(c_1,c_2).
\end{aligned}$$

Donc, $*$ est associative.
— Pour tous $(a_1,a_2),(b_1,b_2),(c_1,c_2) \in \mathbb{Z}^2$, on a

$$\begin{aligned}
(a_1,a_2)*\Big((b_1,b_2)+(c_1,c_2)\Big) &= (a_1,a_2)*(b_1+c_1, b_2+c_2)\\
&= \Big(a_1(b_1+c_1)+2a_2(b_2+c_2), a_1(b_2+c_2)+a_2(b_1+c_1)\Big)\\
&= (a_1b_1+a_1c_1+2a_2b_2+2a_2c_2, a_1b_2+a_1c_2+a_2b_1+a_2c_1)\\
&= (a_1b_1+2a_2b_2, a_1b_2+a_2b_1)+(a_1c_1+2a_2c_2, a_1c_2+a_2c_1)\\
&= (a_1,a_2)*(b_1,b_2)+(a_1,a_2)*(c_1,c_2).
\end{aligned}$$

Donc, $*$ est distributive par rapport à $+$.
Par conséquent, $(\mathbb{Z}^2, +, *)$ est un anneau commutatif unitaire d'élément neutre $(1,0)$.

(2) Montrons que $\mathbb{Z}^2 \cong \mathbb{Z}[\sqrt{2}]$: Rappelons que $\mathbb{Z}\left[\sqrt{2}\right] = \left\{a+b\sqrt{2} \mid a,b\in\mathbb{Z}\right\}$.
On considère l'application $f : \mathbb{Z}^2 \to \mathbb{Z}[\sqrt{2}]$ définie par $f(a,b) = a+b\sqrt{2}$. On a
— $f(0,0) = 0$ et $f(1_{\mathbb{Z}^2}) = f(1,0) = 1$.
— Pour tous $(a,b),(c,d) \in \mathbb{Z}^2$, on a

$$f\Big((a,b)+(c,d)\Big) = f(a+c, b+d) = (a+c)+(b+d)\sqrt{2} = (a+b\sqrt{2})+(c+d\sqrt{2}) = f(a,b)+f(c,d).$$

Scanned with CamScanner

— Pour tous $(a,b),(c,d)\in\mathbb{Z}^2$, on a

$$f\Big((a,b)*(c,d)\Big)=f((ac+2bd,ad+bc))=(ac+2bd)+(ad+bc)\sqrt{2}=(a+b\sqrt{2})(c+d\sqrt{2})=f(a,b).f(c,d).$$

Donc, f est un morphisme d'anneaux de $(\mathbb{Z}^2,+,*)$ vers $(\mathbb{Z}\left[\sqrt{2}\right],+,.)$.
De plus, pour tous $a,b\in\mathbb{Z}$, $a+b\sqrt{2}=0$ implique que $a=b=0$. Donc,

$$\ker(f)=\{(a,b)\mid a+b\sqrt{2}=0\}=\{(0,0\}.$$

Ainsi, f est injective.
Aussi, il est clair que f est surjective par construction.
Par conséquent, f est un isomorphisme (morphisme bijective). D'où le résultat.

Exercice 2. Soit $A=\left\{\frac{m}{n}\mid m\in\mathbb{Z},\ n\in 2\mathbb{Z}+1\right\}$ (c'est-à-dire que A est l'ensemble des rationnels à dénominateur impair).

(1) Démontrer que A est un sous anneau de $(\mathbb{Q},+,\times)$.
(2) Quels sont ses éléments inversibles ?

Solution.

(1) Démontrons que A est un sous anneau de $(\mathbb{Q},+,\times)$: Rappelons qu'une partie A de l'anneau B est un sous-anneau de B si et seulement si :
— $1_B\in A$.
— pour tous $a,b\in A$, $a-b\in A$.
— pour tous $a,b\in A$, $ab\in A$.
Dans notre cas :
— $A\subseteq\mathbb{Q}$.
— $1=\frac{1}{1}\in A$.
— pour tous $\frac{m}{n},\frac{m'}{n'}\in A$ avec n et n' impair, on a nn' est impair et donc

$$\frac{m}{n}-\frac{m'}{n'}=\frac{mn'-m'n}{nn'}\in A \text{ et } \frac{m}{n}.\frac{m'}{n'}=\frac{mm'}{nn'}\in A.$$

Donc, A est un sous-anneau de $(\mathbb{Q},+,\times)$.

(2) Les éléments inversibles de A : Soit $\frac{m}{n}\in U(A)$ (n impair). Il existe $\frac{m'}{n'}\in A$ (n' impair) tel que $\frac{m}{n}.\frac{m'}{n'}=\frac{mm'}{nn'}=1$. Le fait que $mm'=nn'$ implique que m et m' sont impairs. Ainsi,

$$U(A)\subseteq\left\{\frac{m}{n}\mid m,n\in 2\mathbb{Z}+1\right\}.$$

Inversement, si $m,n\in 2\mathbb{Z}+1$ alors $\frac{m}{n}$ est inversible d'inverse $\frac{n}{m}\in A$. Par suite

$$U(A)=\left\{\frac{m}{n}\mid m,n\in 2\mathbb{Z}+1\right\}.$$

Exercice 3. On considère $\mathbb{Z}\left[\sqrt{2}\right]=\left\{a+b\sqrt{2}\mid a,b\in\mathbb{Z}\right\}$.

Scanned with CamScanner

(1) Montrer que $\left(\mathbb{Z}\left[\sqrt{2}\right], +, \times\right)$ est un anneau.

(2) On note $N\left(a + b\sqrt{2}\right) = a^2 - 2b^2$. Montrer que, pour tous x et y de $\mathbb{Z}\left[\sqrt{2}\right]$, on a $N(xy) = N(x)N(y)$.

(3) En déduire que les éléments inversibles de $\mathbb{Z}\left[\sqrt{2}\right]$ sont ceux s'écrivant $a + b\sqrt{2}$ avec $a^2 - 2b^2 = \pm 1$.

Solution.

(1) Montrons que $\left(\mathbb{Z}\left[\sqrt{2}\right], +, \times\right)$ est un anneau.
Il suffit de montrer que $\left(\mathbb{Z}\left[\sqrt{2}\right], +, \times\right)$ est un sous anneau de $(\mathbb{R}, +, \times)$.

(2) On note $N\left(a + b\sqrt{2}\right) = a^2 - 2b^2$. Montrons que, pour tous x et y de $\mathbb{Z}\left[\sqrt{2}\right]$, on a $N(xy) = N(x)N(y)$.
On pose $x = a + b\sqrt{2}$ et $y = c + d\sqrt{2}$ avec $a, b, c, d \in \mathbb{Z}$. Alors,

$$\begin{aligned} N(xy) &= N\left((ac + 2bd) + (ad + bc)\sqrt{2}\right) \\ &= (ac + 2bd)^2 - 2(ad + bc)^2 \\ &= a^2c^2 + 4b^2d^2 + 4abcd - 2a^2d^2 - 2b^2c^2 - 4abcd \\ &= a^2(c^2 - 2d^2) - 2b^2(c^2 - 2d^2) \\ &= (a^2 - 2b^2)(c^2 - 2d^2) \\ &= N(x)N(y). \end{aligned}$$

(3) Déduisons que les éléments inversibles de $\mathbb{Z}\left[\sqrt{2}\right]$ sont ceux s'écrivant $a + b\sqrt{2}$ avec $a^2 - 2b^2 = \pm 1$.
Soit $x = a + b\sqrt{2}$ un élément inversible de $\mathbb{Z}\left[\sqrt{2}\right]$. Il existe $y \in \mathbb{Z}\left[\sqrt{2}\right]$ tel que $xy = 1$. D'où, $N(x)N(y) = N(xy) = N(1) = 1$. Or, $N(x)$ et $N(y$ sont des entiers et donc $N(x) = \pm 1$.
Inversement, si $a^2 - 2b^2 = \pm 1$ alors $(a + b\sqrt{2})(a - \sqrt{2}b) = \pm 1$. Donc, $a + b\sqrt{2}$ est inversible.

Exercice 4 (Anneau de Boole)**.** On dit qu'un anneau A non réduit à $\{0\}$ est un anneau de Boole si, pour tout $x \in A$, on a $x^2 = x$. On fixe A un tel anneau.

(1) Montrer que $(\forall x, y \in A)$, on a $xy + yx = 0$. En déduire que, pour tout $x \in A$, on a $x = -x$.

(2) Montrer que A est commutatif.

(3) Montrer que $(\forall x, y \in A)$, on a $xy(x + y) = 0$. En déduire qu'un anneau de Boole intègre ne peut avoir que deux éléments.

Solution.

(1) Montrons que $(\forall x, y \in A)$, on a $xy + yx = 0$:
On a $(x + y)^2 = x^2 + xy + yx + y^2$. Or $x^2 = x$, $y^2 = y$ et $(x + y)^2 = x + y$ car A est un anneau de Boole. Donc, $x + xy + yx + y = x + y$. Ainsi, $xy + yx = 0$.
Déduction : Pour $x = y$, on obtient $x^2 + x^2 = 0$. Donc, $x + x = 0$, et ainsi, $x = -x$.

(2) Montrons que A est commutatif : Pour tous $x, y \in A$, on a $xy = -yx$. Or, $-yx = yx$. Donc, $xy = yx$. Par suite, A est commutatif.

Scanned with CamScanner

(3) Montrons que $(\forall x, y \in A)$, on a $xy(x+y) = 0$: On a

$$xy(x+y) = xyx + xy^2 = x^2y + xy^2 = xy + yx = 0.$$

Déduction : Soit A un anneau de Boole intègre. Soit $x, y \in A$ avec $x \neq 0$ et $y \neq 0$. Donc, $xy \neq 0$ car A est intègre. Mais $xy(x+y) = 0$, et donc $x + y = 0$. Ainsi, $x = -y = y$. Par conséquent, A contient un seul élément non nul.

Exercice 5. Pour tout $a \in \mathbb{R}$, on pose $I_a = \{P \in \mathbb{R}[X] \mid P(a) = 0\}$.

(1) Montrer que I_a est un ideal de $\mathbb{R}[X]$.

(2) Montrer que si $a \neq b$, alors $I_a + I_b = \mathbb{R}[X]$.

Solution.

(1) Montrons que I_a est un ideal de $\mathbb{R}[X]$:

— Pour tous $P, Q \in I_a$, on a $(P+Q)(a) = P(a) + Q(a) = 0 + 0 = 0$. Donc, $P + Q \in I_a$.
— Pour tous $P \in \mathbb{R}[X]$ et $Q \in I_a$, on a $(PQ)(a) = P(a)Q(a) = P(a).0 = 0$. Donc, $PQ \in I_a$.
Par suite, I_a est un idéal de $\mathbb{R}[X]$.

(2) Montrons que si $a \neq b$, alors $I_a + I_b = \mathbb{R}[X]$:
$I_a + I_b$ est un idéal de $\mathbb{R}[X]$. Comme $P = \dfrac{X-a}{b-a} \in I_a$ et $Q = \dfrac{X-b}{a-b} \in I_b$, alors

$$P + Q = \frac{X - a + b - X}{b - a} = 1 \in I_a + I_b.$$

Donc, $I_a + I_b = \mathbb{R}[X]$.

Exercice 6. Soit A un anneau et e un idempotent (c-à-d, $e^2 = e$).

(1) Montrer que $1 - e$ est encore idempotent.

(2) Montrer que eA et $(1-e)A$ sont des idéaux étrangers dans A.

(3) En déduire que $A \cong A/eA \times A/(1-e)A$.

Solution.

(1) Montrons que $1 - e$ est un idempotent : On a $(1-e)^2 = 1 - 2e + e^2 = 1 - 2e + e = 1 - e$. Donc, $1 - e$ est un idempotent.

(2) Montrons que eA et $(1-e)A$ sont des idéaux étrangers dans A : On a $1 = e + (1-e) \in eA + (1-e)A$. Donc, $eA + (1-e)A = A$. D'où le résultat.

(3) Déduisons que $A \cong A/eA \times A/(1-e)A$: On considère l'application $f : A \to A/eA \times A/(1-e)A$ définie par $f(x) = (\overline{x}, \widehat{x})$. Il est facile de vérifier que f est un morphisme d'anneaux.
Soit $x \in \ker(f)$. Donc, $(\overline{x}, \widehat{x}) = (\overline{0}, \widehat{0})$. Ainsi, $x \in eA \cap (1-e)A$. Donc, il existe $y, z \in A$ tels que $x = ey = (1-e)z$. D'où, $ey = e^2y = e(1-e)z = 0$. Alors, $x = 0$. Par suite, $\ker(f) = \{0\}$, et f est injective.
Soit $(\overline{y}, \widehat{z}) \in A/eA \times A/(1-e)A$. On pose $x = (1-e)y + ez$. On a $\overline{x} = \overline{y}$ et $\widehat{x} = \widehat{z}$. Donc, $f(x) = (\overline{x}, \widehat{x}) = (\overline{y}, \widehat{z})$. Alors, f est surjective.
Par conséquent, f est un isomorphisme d'anneaux. D'où le résultat.

Scanned with CamScanner

Exercice 7. On considère l'anneau $\mathbb{Z}[X]$ des polynômes à coefficients dans $\mathbb{Z}$. On note $(2, X) := 2\mathbb{Z}[X] + X\mathbb{Z}[X]$ l'idéal de $\mathbb{Z}[X]$ engendré par 2 et X.

(1) Montrer que $(2, X)$ n'est pas principal.

(2) Montrer que l'application $f : \mathbb{Z}[X] \to \mathbb{Z}/2\mathbb{Z}$ définie par $f(P) = \overline{P(0)}$ est un morphisme d'anneaux surjectif.

(3) Montrer que $\ker(f) = (2, X)$.

(4) En déduire que $\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}$

(5) Que peut-on dire de l'idéal $(2, X)$?

Solution.

(1) Montrons que $(2, X)$ n'est pas principal : On suppose par l'absurde que $(2, X)$ est principal engendré par un polynôme $P(X) \in \mathbb{Z}[X]$. Donc, il existe $Q \in \mathbb{Z}[X]$ tel que $2 = P(X)Q(X)$. Comme $\mathbb{Z}[X]$ est intègre, $0 = \mathbf{deg}(2) = \mathbf{deg}(P) + \mathbf{deg}(Q)$. Donc, $\mathbf{deg}(P) = \mathbf{deg}(Q) = 0$. Ainsi, $P \in \mathbb{Z}$ et divise 2. Par suite, $P \in \{\pm 1, \pm 2\}$. En outre, il existe $R \in \mathbb{Z}[X]$ tel que $X = PR$. Le coefficient dominant de X qu'est 1 est le produit des coefficients dominants de P (qu'est P) et de R. Donc, P divise 1. Par suite, $P = \pm 1$.
Maintenant $(2, X) = (1)$, et donc il existe $Q, R \in \mathbb{Z}[X]$ tels que $1 = 2Q(X) + XR(X)$. Pour $X = 0$, on obtient $1 = 2Q(0)$, et donc 2 divise 1 ce qu'est absurde. Par conséquent, $(2, X)$ n'est pas principal.

(2) Montrons que l'application $f : \mathbb{Z}[X] \to \mathbb{Z}/2\mathbb{Z}$ définie par $f(P) = \overline{P(0)}$ est un morphisme d'anneaux surjectif :
Il est clair que $f(0) = \overline{0}$, $f(1) = \overline{1}$, $f(P + Q) = f(P) + f(Q)$ et $f(PQ) = f(P)f(Q)$.
En plus, les deux première égalités veulent dire tout simplement que f est surjective.

(3) Montrons que $\ker(f) = (2, X)$: On a $f(2) = \overline{2} = \overline{0}$ et $f(X) = \overline{0}$. Donc, $2 \in \ker(f)$ et $X \in \ker(f)$. Alors, $(2, X) \subseteq \ker(f)$.
Inversement, soit $P = \sum_{i=0}^{n} a_i X^i \in \ker(f)$. Donc, $\overline{a_0} = \overline{P(0)} = \overline{0}$. Ainsi, $a_0 \in 2\mathbb{Z}$. Posons $a_0 = 2a_0'$ avec $a_0' \in \mathbb{Z}$. On alors, $P(X) = 2a_0' + X(\sum_{i=1}^{n} a_i X^{i-1}) \in (2, X)$. Par suite, $\ker(f) \subseteq (2, X)$. D'où l'égalité désirée.

(4) Déduisons que $\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}$: D'après le premier théorème d'isomorphisme, on a $\mathbb{Z}[X]/\ker(f) \cong \mathrm{Im}(f)$. Comme f est surjective, $\mathrm{Im}(f) = \mathbb{Z}/2\mathbb{Z}$. En plus, $\ker(f) = (2, X)$. Donc, on obtient que $\mathbb{Z}[X]/(2, X) \cong \mathbb{Z}/2\mathbb{Z}$.

(5) Que peut-on dire de l'idéal $(2, X)$? L'anneau $\mathbb{Z}/2\mathbb{Z}$ est un corps. Donc, $(2, X)$ est un idéal maximal de $\mathbb{Z}[X]$.

Exercice 8 (Idéaux premiers)**.**

(1) Montrer que les idéaux premiers non nuls de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ avec p un entier premier.

(2) Soit $P \in \mathbb{R}[X]$ un polynôme irréductible. Montrer que $P\mathbb{R}[X] = \{PQ \mid Q \in \mathbb{R}[X]\}$ est idéal premier de $\mathbb{R}[X]$.

Scanned with CamScanner

(3) Soit A un anneau commutatif dont tout idéal est premier. Etablir que A est intègre puis que A est un corps.

Solution.

(1) Montrons que les idéaux premiers non nuls de $\mathbb{Z}$ sont de la forme $p\mathbb{Z}$ avec p un entier premier : Soit I un idéal non nul de $\mathbb{Z}$. L'idéal I contient un élément non nul m. Si m n'est pas positif, alors I contient aussi $-m$ qu'est maintenant positif. En tou cas I contient un entier positif non nul m. Soit n le plus petit entier positif dans I. Soit $m \in I$ positif. En faisant le division de m par n, on obtient $m = nq + r$ avec $q, r \in \mathbb{N}$ et $r < n$. Or, $r = m - qn \in I$. Donc, par minimalité de n, on obtient $r = 0$. Donc, $m \in n\mathbb{Z}$. Soit $m \in I$ négatif. Alors, $-m \in I$ est positif, et donc $-m \in n\mathbb{Z}$. Alors, $m \in n\mathbb{Z}$. Par suite, $I \subseteq n\mathbb{Z} \subseteq I$. D'où $I = n\mathbb{Z}$.
On conclut alors que les idéaux de $\mathbb{Z}$ sont de la forme $n\mathbb{Z}$ avec n un entier positif.
Soit $n\mathbb{Z}$ un idéal non nul de Z. Alors, $n\mathbb{Z}$ est premier si et seulement si $\mathbb{Z}/n\mathbb{Z}$ est intègre si et seulement si n est un entier premier.

(2) Soit $P \in \mathbb{R}[X]$ un polynôme irréductible. Montrons que $P\mathbb{R}[X] = \{PQ \mid Q \in \mathbb{R}[X]\}$ est idéal premier de $\mathbb{R}[X]$: Il est clair que $P\mathbb{R}[X]$ est un idéal principal. Soient $Q, R \in \mathbb{R}[X]$ tels que $QR \in P\mathbb{R}[X]$. Donc, P divise QR. Comme P est irréductible, on a soit P divise Q soit P divise R. Alors, $Q \in P\mathbb{R}[X]$ ou $R \in P\mathbb{R}[X]$. D'où, $P\mathbb{R}[X]$ est un idéal premier de $\mathbb{R}[X]$.

(3) Soit A un anneau commutatif dont tout idéal est premier. Montrons que A est un corps :
Comme $\{0\}$ est premier, alors A est intègre. Soit maintenant $x \in A$ non nul. On a $x^2 \in (x^2)$. Or, (x^2) est premier ce qui implique que $x \in (x^2)$. Alors, $x = rx^2$ pour un certain $r \in A$. D'où, $x(1 - rx) = 0$. Par suite, $1 = rx$, et alors x est inversible. Par conséquent, A est un corps.

Exercice 9. Soient A et B deux anneaux commutatifs.

(1) Montrer que les idéaux de $A \times B$ sont exactemenet les ensembles $I \times J$ avec I un idéal de A et J un idéal de B.

(2) Montrer qu'un idéal premier de $A \times B$ est de la forme $P \times B$ avec P un idéal premier de A ou de la forme $A \times Q$ ou Q est un ideal premier de B.

(3) Montrer qu'un idéal maximal de $A \times B$ est de la forme $P \times B$ avec P un idéal maximal de A ou de la forme $A \times Q$ ou Q est un ideal maximal de B.

(4) On suppose que A et B sont des corps. Donner tous les idéaux maximaux de $A \times B$.

Solution.

(1) Montrons que les idéaux de $A \times B$ sont exactement les ensembles $I \times J$ avec I un idéal de A et J un idéal de B :
Il est facile de voir que si I un idéal de A et J un idéal de B alors $I \times J$ est un idéal de $A \times B$.
Soit K un idéal de $A \times B$. On pose $I = \{x \in A \mid \text{ il existe } y \in B \text{ tel que } (x, y) \in K\}$ et $J = \{y \in B \mid \text{ il existe } x \in A \text{ tel que } (x, y) \in K\}$. Il est clair que I et J sont non vides.
Soient $x, x' \in I$. Il existe $y, y' \in B$ tels que $(x, y) \in K$ et $(x', y') \in K$. Donc, $(x + x', y + y') \in K$. Alors, $x + x' \in I$. En plus, pour tout $a \in A$, on $(ax, 0) = (a, 0)(x, y) \in K$. Donc, $ax \in I$.

Scanned with CamScanner

Par suite, I est idéal de A. De même, J est idéal de B.
Soient, $x \in I$ et $y \in J$. Il existe $y_0 \in B$ et $x_0 \in A$ tels que $(x, y_0) \in K$ et $(x_0, y) \in K$. Donc,

$$(x, y) = (1, 0)(x, y_0) + (0, 1)(x_0, y) \in K.$$

D'où, $I \times J \subseteq K$. L'autre inclusion est triviale. Par suite, $K = I \times J$.

(2) Montrons qu'un idéal premier de $A \times B$ est de la forme $P \times B$ avec P un idéal premier de A ou de la forme $A \times Q$ ou Q est un ideal premier de B : Soient $K = I \times J$ un idéal premier de $A \times B$. Supposons $I \neq A$. Il existe $a \in A$ et $a \notin I$. Pour tout $b \in B$, on a $(a, 0)(0, b) = (0, 0) \in I \times J$. Mais $(a, 0) \notin I \times J$. Donc, $(0, b) \in I \times J$, et donc $b \in J$. Par suite, $J = B$. Donc, $K = I \times B$. De même si $J \neq B$, on obtient $I = A$ et donc $K = A \times J$.
En plus, il est facile de vérifier que l'application $f : A \times B/I \times B \to A/I$ définie par $f\left(\overline{(a, b)}\right) = \widehat{a}$ est un isomorphisme d'anneaux. Donc, $A \times B/I \times B \cong A/I$. De même, pour un idéal J de B, on a $A \times B/A \times J \cong B/J$.
Ainsi, $I \times B$ est premier si et seulement si $A \times B/I \times B \cong A/I$ est intègre si et seulement si I est premier. Par analogie, $A \times J$ est premier si et seulement si J est premier.

(3) Montrons qu'un idéal maximal de $A \times B$ est de la forme $P \times B$ avec P un idéal maximal de A ou de la forme $A \times Q$ ou Q est un ideal maximal de B : Soit K un idéal maximal de $A \times B$. De la question précédente, $K = I \times B$ ou $K = A \times J$.
Ainsi, $I \times B$ est maximal si et seulement si $A \times B/I \times B \cong A/I$ est un corps si et seulement si I est maximal. Par analogie, $A \times J$ est maximal si et seulement si J est maximal.

(4) On suppose que A et B sont des corps. Les idéaux maximaux de $A \times B$ sont $A \times \{0_B\}$ et $\{0_A\} \times B$.

Exercice 10. Soit A un anneau commutatif unitaire.

(1) On suppose que A n'admet que les idéaux triviaux $\{0\}$ et A. Démontrer que A est un corps.

(2) On suppose que A est intègre et qu'il n'admet qu'un nombre fini d'idéaux. Démontrer que A est un corps.

(3) En déduire que tout anneau commutatif unitaire intègre fini est un corps.

Solution.

(1) On suppose que A n'admet que les idéaux triviaux $\{0\}$ et A. Démontrons que A est un corps.
Soit $x \in A$ non nul. Alors, $(x) = A$ car (x) est un idéal non nul. Donc, $1 \in (x)$. Alors, il existe $a \in A$ tel que $ax = 1$. D'où x est inversible. Par conséquent, A est un corps.

(2) On suppose que A est intègre et qu'il n'admet qu'un nombre fini d'idéaux. Démontrons que A est un corps.
Soit $x \in A$ non nul. Pour tout $n \geq 1$, (x^n) est un idéal de A. Mais A ne contient qu'un nombre fini d'idéaux et donc il existe $n, m \geq 1$ tels que $n > m$ et $(x^n) = (x^m)$. Donc, $x^m \in (x^n)$. Alors, il existe $a \in A$ tel que $x^m = ax^n$. Donc, $x^m(1 - ax^{n-m}) = 0$. Comme A est intègre, on obtient $1 = ax^n$. Donc, x est inversible. Par suite, A est un corps.

(3) Déduisons que tout anneau commutatif unitaire intègre fini est un corps.
Un anneau fini contient un nombre fini d'idéaux. Donc, un anneau commutatif unitaire intègre fini est un corps.

Scanned with CamScanner

Série 2

Anneaux euclidiens et principaux : divisibilité et arithmétique.

Exercice 1. On se place dans l'anneau euclidien des entiers de Gauss $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$. Pour $z = a + ib \in \mathbb{Z}[i]$, on définit $N(z) = |z|^2 = a^2 + b^2$.

(1) En utilisant le fait que $N(xy) = N(x)N(y)$, déterminer tous les inversibles de $\mathbb{Z}[i]$.

(2) Montrer que si $N(z)$ est un nombre premier alors z est irreductible dans $\mathbb{Z}[i]$.

(3) Montrer que pour tout $z \in \mathbb{Z}[i]$, on a $N(z) \neq 3$. En déduire que 3 est irreductible dans $\mathbb{Z}[i]$.

(4) Montrer que 5 n'est pas un irreductible dans $\mathbb{Z}[i]$.

(5) Soit z un élément irréductible de $\mathbb{Z}[i]$. Montrer que l'anneau quotient $\mathbb{Z}[i]/(z)$ est un corps.

Exercice 2. On se place dans l'anneau $\mathbb{Z}\left[\sqrt{10}\right] = \left\{a + \sqrt{10}b \mid a, b \in \mathbb{Z}\right\}$.

(1) Montrer que $a + \sqrt{10}b$ est inversible dans $\mathbb{Z}\left[\sqrt{10}\right]$ si et seulement si $a^2 - 10b^2 = \pm 1$.

(2) Montrer que l'équation $a^2 - 10b^2 = 2$ n'a pas de solutions dans $\mathbb{Z}$.

(3) En déduire que 2 est irreductible dans l'anneau $\mathbb{Z}\left[\sqrt{10}\right]$.

(4) En écrivant 10 de deux facons différentes dans $\mathbb{Z}\left[\sqrt{10}\right]$, montrer que 2 n'est pas premier.

(5) En déduire que l'anneau $\mathbb{Z}\left[\sqrt{10}\right]$ n'est pas principal.

Exercice 3. On considère l'anneau $\mathbb{Z}[i\sqrt{5}] = \left\{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$ sur lequel on définit l'application N donnée par $N(a + bi\sqrt{5}) = |a + bi\sqrt{2}|^2 = a^2 + 5b^2$.

(1) Vérifier que N est multiplicative (c-à-d, $N(xy) = N(x)N(y)$ pour tous $x, y \in \mathbb{Z}[i\sqrt{5}]$) et que $N(x) = 0$ si et seulement si $x = 0$.

(2) Déterminer les éléments inversibles de $\mathbb{Z}[i\sqrt{5}]$.

(3) Montrer que 2 est irréductible mais que 2 n'est pas premier [On pourra utiliser $6 = (1 - i\sqrt{5})(1 + i\sqrt{5})$].

(4) Que peut-on dire de l'anneau $\mathbb{Z}[i\sqrt{5}]$?

Exercice 4. On considère l'anneau $\mathbb{Z}[i\sqrt{2}] = \left\{a + bi\sqrt{2} \mid a, b \in \mathbb{Z}\right\}$ sur lequel on définit l'application norme N donnée par $N(a + bi\sqrt{2}) = |a + bi\sqrt{2}|^2 = a^2 + 2b^2 \in \mathbb{N}$.

(1) Vérifier que N est multiplicative (c-à-d, $N(xy) = N(x)N(y)$ pour tous $x, y \in Z[i\sqrt{2}]$)

(2) Déterminer les éléments inversibles de $\mathbb{Z}[i\sqrt{2}]$.

(3) Soit $x \in \mathbb{Z}[i\sqrt{2}]$. Montrer que si $N(x)$ est un nombre premier alors x est irreductible dans $\mathbb{Z}[i\sqrt{2}]$.

(4) Soient $x, y \in \mathbb{Z}[i]$ avec $y \neq 0$.

(a) Montrer qu'il existe $q \in \mathbb{Z}[i\sqrt{2}]$ tel que $\left|q - \dfrac{x}{y}\right| < 1$.

Scanned with CamScanner

(b) On pose $r = x - qy$. Vérifier que $|r| < |y|$.

(c) Conclure que l'anneau $\mathbb{Z}[i\sqrt{2}]$ est Euclidien.

(5) Donner tous les diviseurs de $2 + i\sqrt{2}$ dans $\mathbb{Z}[i\sqrt{2}]$.

(6) Donner la liste des diviseurs communs de $2 + i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$.

(7) Donner tous les pgcd de $2 + i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$

Exercice 5. On définit la norme de $z = x + yi \in \mathbb{C}$ par $N(z) = z\overline{z} = x^2 + y^2$.

(1) Soit p un nombre premier. Montrer que les assertions suivantes sont équivalentes :

(a) p est irréductible dans $\mathbb{Z}[i]$.

(b) $p \equiv 3\ [4]$.

(c) il n'existe pas $a \in \mathbb{Z}[i]$ tel que $p = N(a)$.
On admettra que —1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si p n'est pas congru à 3 modulo 4.

(2) En déduire tous les irréductibles de $\mathbb{Z}[i]$.

(3) Parmi les éléments $1 + i, 2 + i, 2, 3, 5 \in \mathbb{Z}[i]$ lesquels sont irréductibles dans $\mathbb{Z}[i]$?

Scanned with CamScanner

Série 2 : Correction

Anneaux euclidiens et principaux : divisibilité et arithmétique.

Exercice 1. On se place dans l'anneau euclidien des entiers de Gauss $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$. Pour $z = a + ib \in \mathbb{Z}[i]$, on définit $N(z) = |z|^2 = a^2 + b^2$.

(1) En utilisant le fait que $N(xy) = N(x)N(y)$, déterminer tous les inversibles de $\mathbb{Z}[i]$.

(2) Montrer que si $N(z)$ est un nombre premier alors z est irreductible dans $\mathbb{Z}[i]$.

(3) Montrer que pour tout $z \in \mathbb{Z}[i]$, on a $N(z) \neq 3$. En déduire que 3 est irréductible dans $\mathbb{Z}[i]$.

(4) Montrer que 5 n'est pas un irréductible dans $\mathbb{Z}[i]$.

(5) Soit z un élément irréductible de $\mathbb{Z}[i]$. Montrer que l'anneau quotient $\mathbb{Z}[i]/(z)$ est un corps.

Solution.

(1) En utilisant le fait que $N(xy) = N(x)N(y)$, déterminons tous les inversibles de $\mathbb{Z}[i]$:
Soit $z = a + ib \in U\big(\mathbb{Z}[i]\big)$. Il existe $z' \in \mathbb{Z}[i]$ tel que $zz' = 1$. Donc, $N(z)N(z') = 1$. Comme $N(z), N(z') \in \mathbb{N}$, on obtient $N(z) = 1$. Donc, $a^2 + b^2 = 1$. Par suite, $(a, b) = (1, 0)$ ou $(a, b) = (-1, 0)$ ou $(a, b) = (0, 1)$ ou $(a, b) = (0, -1)$. C'est à dire, $z = \pm 1$ ou $z = \pm i$.
Inversement, 1 et -1 sont inversible et i et $-i$ sont aussi inversible car $i \times (-i) = 1$.
Enfin,
$$z \in U\big(\mathbb{Z}[i]\big) \Leftrightarrow N(z) = 1 \Leftrightarrow z \in \{1, -1, i, -i\}.$$

(2) Montrons que si $N(z)$ est un nombre premier alors z est irréductible dans $\mathbb{Z}[i]$:
Soit $z \in \mathbb{Z}[i]$ tel que $N(z) = p$ un entier premier.
— $z \neq 0$ (sinon $N(z) = 0$).
— $z \notin \mathbb{Z}[i]$ car $N(z) \neq 1$ (rappelez-vous que 1 n'est pas un entier premier).
— Soient $z_1, z_2 \in \mathbb{Z}[i]$ tels que $z = z_1 z_2$. Donc, $p = N(z) = N(z_1)N(z_2)$. Comme p est premier, on a nécessairement $N(z_1) = 1$ ou $N(z_2) = 1$. Donc, z_1 est inversible ou z_2 est inversible.
On en déduit donc que z est irréductible.

(3) Montrons que pour tout $z \in \mathbb{Z}[i]$, on a $N(z) \neq 3$ et déduisons que 3 est irreductible dans $\mathbb{Z}[i]$:
Soit $z = a + ib \in \mathbb{Z}[i]$. Supposons que $N(z) = 3$. Donc, $a^2 + b^2 = 3$. Ainsi,
— $a^2 = 0$ et $b^2 = 3$, ou
— $a^2 = 1$ et $b^2 = 2$, ou
— $a^2 = 2$ et $b^2 = 1$, ou
— $a^2 = 3$ et $b^2 = 0$.
Tous les cas sont impossibles car $\sqrt{3} \notin \mathbb{Z}$ et $\sqrt{2} \notin \mathbb{Z}$. Donc, notre hypothèse est fausse. Par suite, $N(z) \neq 3$.

Déduisons que 3 est irréductible :
— $3 \neq 0$.
— $3 \notin U\big(\mathbb{Z}[i]\big)$.
— Soient $z_1, z_2 \in \mathbb{Z}[i]$ tels que $3 = z_1 z_2$. Donc, $9 = N(3) = N(z_1)N(z_2)$. Comme $N(z_1) \neq 3$ et $N(z_2) \neq 3$, on a nécessairement $N(z_1) = 1$ ou $N(z_2) = 1$. Donc, z_1 est inversible ou z_2 est inversible.

Scanned with CamScanner

(4) Montrons que 5 n'est pas un irréductible dans $\mathbb{Z}[i]$:
On a $5 = (2+i)(2-i)$ et $2+i, 2-i \notin U\Big(\mathbb{Z}[i]\Big)$. Donc, 5 n'est pas un irréductible dans $\mathbb{Z}[i]$.

(5) Soit z un élément irréductible de $\mathbb{Z}[i]$. Montrons que l'anneau quotient $\mathbb{Z}[i]/(z)$ est un corps :
L'anneau $\mathbb{Z}[i]$ est euclidien, et donc principal. Ainsi, tout élément irréductible de $\mathbb{Z}[i]$ est premier. Par suite, z est premier, et donc l'idéal principal (z) de $\mathbb{Z}[i]$ est premier. On en déduit alors que l'anneau quotient $\mathbb{Z}[i]/(z)$ est intègre.
Soit $\overline{x} = \overline{a+ib} \in \mathbb{Z}[i]/(z)$. En effectuant la division euclidienne de x par z, on obtient $x = yz + r$ avec $y, r \in \mathbb{Z}[i]$ et $r = 0$ ou $N(r) < N(z) = a^2 + b^2$. Donc, $\overline{x} = \overline{0}$ ou $\overline{x} = \overline{r}$. On pose $r = a_0 + ib_0$. Donc, $a_0^2 + b_0^2 = N(r) < N(z) = a^2 + b^2$. Donc, $a_0 < \sqrt{a^2+b^2}$ et $b_0 < \sqrt{a^2+b^2}$. Donc,

$$\mathbb{Z}[i]/(z) = \{a_0 + ib_0 \mid a_0, b_0 \in \mathbb{Z}, \quad a_0 < \sqrt{a^2+b^2} \quad \text{et} \quad b_0 < \sqrt{a^2+b^2}\}.$$

L'anneau quotient $\mathbb{Z}[i]/(z)$ est donc fini. Nous savons qu'un anneau intègre fini est un corps. Par conséquent, l'anneau quotient $\mathbb{Z}[i]/(z)$ est un corps.

Exercice 2. On se place dans l'anneau $\mathbb{Z}\Big[\sqrt{10}\Big] = \Big\{a + \sqrt{10}b \mid a, b \in \mathbb{Z}\Big\}$.

(1) Montrer que $a + \sqrt{10}b$ est inversible dans $\mathbb{Z}\Big[\sqrt{10}\Big]$ si et seulement si $a^2 - 10b^2 = \pm 1$.

(2) Montrer que l'équation $a^2 - 10b^2 = \pm 2$ n'a pas de solutions dans $\mathbb{Z}$.

(3) En déduire que 2 est irreductible dans l'anneau $\mathbb{Z}\Big[\sqrt{10}\Big]$.

(4) En écrivant 10 de deux manières différentes dans $\mathbb{Z}\Big[\sqrt{10}\Big]$, montrer que 2 n'est pas premier.

(5) En déduire que l'anneau $\mathbb{Z}\Big[\sqrt{10}\Big]$ n'est pas principal.

Solution.

(1) Montrons que $a + \sqrt{10}b$ est inversible dans $\mathbb{Z}\Big[\sqrt{10}\Big]$ si et seulement si $a^2 - 10b^2 = \pm 1$:
Pour $x = a + \sqrt{10}b \in \mathbb{Z}\Big[\sqrt{10}\Big]$, on définit $N(x) = a^2 - 10b^2$. On montre facilement que N est multiplicative. C'est à dire, pour tous $x, y \in \mathbb{Z}\Big[\sqrt{10}\Big]$, on a $N(xy) = N(x)N(y)$.
Soit $x = a + \sqrt{10}b \in U\Big(\mathbb{Z}\Big[\sqrt{10}\Big]\Big)$. Il existe $y \in \mathbb{Z}\Big[\sqrt{10}\Big]$ tel que $xy = 1$. Donc, $N(x)N(y) = 1$. Comme $N(x), N(y) \in \mathbb{Z}$, on obtient $N(z) = \pm 1$. Donc, $a^2 - 10b^2 = \pm 1$.
Inversement, soit $x = a + \sqrt{10}b \in \mathbb{Z}\Big[\sqrt{10}\Big]$ tel que $a^2 - 10b^2 = \pm 1$.
— Si $a^2 - 10b^2 = 1$, alors $(a + \sqrt{10}b)(a - \sqrt{10}b) = 1$. Donc, $a + \sqrt{10}b$ est inversible d'inverse $a - \sqrt{10}b$.
— Si $a^2 - 10b^2 = -1$, alors $(a + \sqrt{10}b)(-a + \sqrt{10}b) = 1$. Donc, $a + \sqrt{10}b$ est inversible d'inverse $-a + \sqrt{10}b$.
Enfin,

$$U\Big(\mathbb{Z}\Big[\sqrt{10}\Big]\Big) = \{a + \sqrt{10}b \mid a, b \in \mathbb{Z} \text{ et } a^2 - 10b^2 = \pm 1\}.$$

(2) Montrons que l'équation $a^2 - 10b^2 = \pm 2$ n'a pas de solutions dans $\mathbb{Z}$:
Soient $a, b \in \mathbb{Z}$ tels que $a^2 - 10b^2 = \pm 2$. En passant au classes dans l'anneau $\mathbb{Z}/5\mathbb{Z}$, on

Scanned with CamScanner

obtient $\overline{a}^2 = \pm\overline{2}$. Donc, $\overline{a}^2 = \overline{2}$ ou $\overline{a}^2 = -\overline{2} = \overline{3}$. Or les carrés dans $\mathbb{Z}/5\mathbb{Z}$ sont

$$\overline{0}^2 = \overline{0}, \quad \overline{1}^2 = \overline{1}, \quad \overline{2}^2 = \overline{4}, \quad \overline{3}^2 = \overline{9} = \overline{4}, \quad \overline{4}^2 = \overline{16} = \overline{1}.$$

Donc, $\overline{2}$ et $-\overline{2}$ ne sont pas des carrés dans $\mathbb{Z}/5\mathbb{Z}$, et donc a n'existe. Par suite, l'équation $a^2 - 10b^2 = \pm 2$ n'a pas de solutions dans $\mathbb{Z}$.

(3) Déduisons que 2 est irréductible dans l'anneau $\mathbb{Z}\left[\sqrt{10}\right]$:
— $2 \neq 0$.
— $2 \notin U\left(\mathbb{Z}\left[\sqrt{10}\right]\right)$ car $N(2) = 4 \neq \pm 1$.
— Soient $x, y \in \mathbb{Z}[i]$ tels que $2 = xy$. Donc, $4 = N(x)N(y)$. D'après la question précédente, $N(x) \neq \pm 2$ et $N(y) \neq \pm 2$. Donc, on a nécessairement $N(x) = \pm 1$ ou $N(y) = \pm 1$. Donc, x est inversible ou y est inversible.
Par suite, 2 est irréductible dans l'anneau $\mathbb{Z}\left[\sqrt{10}\right]$.

(4) Ecrivant 10 de deux manières différentes dans $\mathbb{Z}\left[\sqrt{10}\right]$, puis montrons que 2 n'est pas premier :
On a

$$10 = 2 \times 5 = (10 + 3\sqrt{10})(10 - 3\sqrt{10}).$$

Supposons que 2 est premier dans $\mathbb{Z}\left[\sqrt{10}\right]$. Donc, puisque 2 divise $(10 + 3\sqrt{10})(10 - 3\sqrt{10})$, on a 2 divise $10 + 3\sqrt{10}$ ou 2 divise $10 - 3\sqrt{10}$.
— Si 2 divise $10 + 3\sqrt{10}$, alors $10 + 3\sqrt{10} = 2(a + b\sqrt{10})$ avec $a, b \in \mathbb{Z}$. Donc, $10 = N(10 + 3\sqrt{10}) = N(2)N((a + b\sqrt{10})) = 4(a^2 - 10b^2)$. Alors, 4 divise 10, ce qu'est absurde.
— De même si 2 divise $10 - 3\sqrt{10}$, on obtient 4 divise 10, ce qu'est absurde.
Par conséquent 2 n'est pas premier dans $\mathbb{Z}\left[\sqrt{10}\right]$.

(5) Déduisons que l'anneau $\mathbb{Z}\left[\sqrt{10}\right]$ n'est pas principal :
Dans un anneau principal tout élément irréductible est premier. Or, dans $\mathbb{Z}\left[\sqrt{10}\right]$, l'élément 2 est irréductible mais pas premier. Donc, $\mathbb{Z}\left[\sqrt{10}\right]$ n'est pas principal.

Exercice 3. On considère l'anneau $\mathbb{Z}[i\sqrt{5}] = \left\{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\right\}$ sur lequel on définit l'application N donnée par $N(a + bi\sqrt{5}) = |a + bi\sqrt{2}|^2 = a^2 + 5b^2$.

(1) Vérifier que N est multiplicative (c-à-d, $N(xy) = N(x)N(y)$ pour tous $x, y \in \mathbb{Z}[i\sqrt{5}]$) et que $N(x) = 0$ si et seulement si $x = 0$.

(2) Déterminer les éléments inversibles de $\mathbb{Z}[i\sqrt{5}]$.

(3) Montrer que 2 est irréductible mais que 2 n'est pas premier [On pourra utiliser $6 = (1 - i\sqrt{5})(1 + i\sqrt{5})$].

(4) Que peut-on dire de l'anneau $\mathbb{Z}[i\sqrt{5}]$?

Solution.

Scanned with CamScanner

(1) Vérifions que N est multiplicative et que $N(x) = 0$ si et seulement si $x = 0$:
Soient $a, b, c, d \in \mathbb{Z}$. On a

$$\begin{aligned} N\Big((a + bi\sqrt{5})(c + di\sqrt{5})\Big) &= N\Big((ac - 5bd) + (ad + bc)i\sqrt{5}\Big) \\ &= (ac - 5bd)^2 + 5(ad + bc)^2 \\ &= a^2b^2 + 25b^2d^2 - 10abcd + 5a^2d^2 + 5b^2c^2 + 10abcd \\ &= a^2(c^2 + 5d^2) + 5b^2(c^2 + 5d^2) \\ &= (a^2 + 5b^2)(c^2 + 5d^2) \\ &= N(a + bi\sqrt{5})N(c + di\sqrt{5}) \end{aligned}$$

En plus,

$$N(a + bi\sqrt{5}) = 0 \Leftrightarrow a^2 + 5b^2 = 0 \Leftrightarrow a = b = 0 \Leftrightarrow a + bi\sqrt{5} = 0.$$

(2) Déterminons les éléments inversibles de $\mathbb{Z}[i\sqrt{5}]$:
Soit $x = a + bi\sqrt{5} \in U\Big(\mathbb{Z}[i\sqrt{5}]\Big)$. Il existe $y \in \mathbb{Z}[i\sqrt{5}]$ tel que $xy = 1$. Donc, $N(x)N(y) = 1$.
Comme $N(x), N(y) \in \mathbb{N}$, on obtient $N(z) = 1$. Donc, $a^2 + 5b^2 = 1$. Ainsi, $a^2 = 1$ et $b^2 = 0$.
Par suite, $a = \pm 1$ et $b = 0$. Donc, $x = \pm 1$.
Inversement, 1 et -1 sont inversibles.
Enfin, $U\Big(\mathbb{Z}[i\sqrt{5}]\Big) = \{1, -1\}$.

(3) Montrons que 2 est irréductible mais que 2 n'est pas premier :
Montrons que 2 est irréductible : On a
— $2 \neq 0$.
— $2 \notin U\Big(\mathbb{Z}[i\sqrt{5}]\Big)$.
— Soient $x, y \in \mathbb{Z}[i\sqrt{5}]$ tels que $2 = xy$. Donc, $4 = N(x)N(y)$. On a $N(x), N(y) \in \mathbb{N}$. Donc, $N(x) \in \{1, 2, 4\}$.
Si $N(x) = 1$ alors $x = 1$, et donc x est inversible.
Si $N(x) = 4$, alors $N(y) = 1$ et donc y est inversible.
Si $N(x) = 2$ alors $a^2 + 5b^2 = 2$. Ainsi, $a^2 = 2$ et $b^2 = 0$, ce qu'est absurde car $\sqrt{2} \notin \mathbb{Z}$.
Donc, nécessairement x est inversible ou y est inversible. Par conséquent, 2 est irréductible.
Montrons que 2 n'est pas premier :
Supposons que 2 est premier dans $\mathbb{Z}[i\sqrt{5}]$. Comme $2 \times 3 = 6 = 6 = (1 - i\sqrt{5})(1 + i\sqrt{5})$, on a 2 divise $1 - i\sqrt{5}$ ou 2 divise $1 + i\sqrt{5}$.
Si 2 divise $1 - i\sqrt{5}$ alors il existe $y \in \mathbb{Z}[i\sqrt{5}]$ tel que $1 - i\sqrt{5} = 2y$. Donc, $N(1 - i\sqrt{5}) = N(2)N(y)$. Ainsi, $6 = 4N(y)$. Par suite, 4 divise 6, ce qu'est absurde.
De même si 2 divise $1 + i\sqrt{5}$ alors il existe $y \in \mathbb{Z}[i\sqrt{5}]$ tel que $1 + i\sqrt{5} = 2y$. Donc, $N(1 + i\sqrt{5}) = N(2)N(y)$. Ainsi, $6 = 4N(y)$. Par suite, 4 divise 6, ce qu'est absurde.
Donc, 2 n'est pas premier.

(4) Que peut-on dire de l'anneau $\mathbb{Z}[i\sqrt{5}]$?
On déduit que $\mathbb{Z}[i\sqrt{5}]$ n'est pas principal. En effet, dans un anneau principal tout élément irréductible est premier.

Exercice 4. On considère l'anneau $\mathbb{Z}[i\sqrt{2}] = \Big\{a + bi\sqrt{2} \mid a, b \in \mathbb{Z}\Big\}$ sur lequel on définit l'application norme N donnée par $N(a + bi\sqrt{2}) = |a + bi\sqrt{2}|^2 = a^2 + 2b^2 \in \mathbb{N}$.

Scanned with CamScanner

(1) Vérifier que N est multiplicative (c-à-d, $N(xy) = N(x)N(y)$ pour tous $x, y \in Z[i\sqrt{2}]$)

(2) Déterminer les éléments inversibles de $\mathbb{Z}[i\sqrt{2}]$.

(3) Soit $x \in \mathbb{Z}[i\sqrt{2}]$. Montrer que si $N(x)$ est un nombre premier alors x est irreductible dans $\mathbb{Z}[i\sqrt{2}]$.

(4) Soient $x, y \in \mathbb{Z}[i\sqrt{2}]$ avec $y \neq 0$.

(a) Montrer qu'il existe $q \in \mathbb{Z}[i\sqrt{2}]$ tel que $\left|q - \frac{x}{y}\right| < 1$.

(b) On pose $r = x - qy$. Vérifier que $|r| < |y|$.

(c) Conclure que l'anneau $\mathbb{Z}[i\sqrt{2}]$ est Euclidien.

(5) Donner tous les diviseurs de $2 + i\sqrt{2}$ dans $\mathbb{Z}[i\sqrt{2}]$.

(6) Donner la liste des diviseurs communs de $2 + i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$.

(7) Donner tous les pgcd de $2 + i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$

Solution.

(1) Vérifions que N est multiplicative : Soient $z, z' \in \mathbb{Z}[i\sqrt{2}]$. On a

$$N(zz') = |zz'|^2 = |z|^2|z'|^2 = N(z)N(z').$$

Donc, N est multiplicative.

(2) Les éléments inversibles de $\mathbb{Z}[i\sqrt{2}]$: Soit $z \in U\left(\mathbb{Z}[i\sqrt{2}]\right)$. Il existe $z' \in \mathbb{Z}[i\sqrt{2}]$ tel que $zz' = 1$. Donc, $N(z)N(z') = 1$. Comme $N(z), N(z') \in \mathbb{N}$, on a nécessairement $N(z) = 1$. Ainsi, $a^2 + 2b^2 = 1$. Par suite, $a = \pm 1$ et $b = 0$.Donc, $z = \pm 1$. Inversement, 1 et -1 sont inversibles. Par conséquent,

$$U(\mathbb{Z}[i\sqrt{2}]) = \{\pm 1\}.$$

(3) Soit $x \in \mathbb{Z}[i\sqrt{2}]$. Montrer que si $N(x)$ est un nombre premier alors x est irréductible dans $\mathbb{Z}[i\sqrt{2}]$:
Soit $z \in \mathbb{Z}[i\sqrt{2}]$ tel que $N(z) = p$ soit un entier premier.
— $z \neq 0$ (sinon $N(z) = 0$).
— $z \notin \mathbb{Z}[i\sqrt{2}]$ car $N(z) \neq 1$ (rappelez-vous que 1 n'est pas un entier premier).
— Soient $z_1, z_2 \in \mathbb{Z}[i\sqrt{2}]$ tels que $z = z_1 z_2$. Donc, $p = N(z) = N(z_1)N(z_2)$. Comme p est premier, on a nécessairement $N(z_1) = 1$ ou $N(z_2) = 1$. Donc, $z_1 = \pm 1$ ou $z_2 = \pm$. Alors, z_1 est inversible ou z_2 est inversible.
On en déduit donc que z est irréductible.

(4) Soient $x, y \in \mathbb{Z}[i\sqrt{2}]$ avec $y \neq 0$.

(a) Montrer qu'il existe $q \in \mathbb{Z}[i\sqrt{2}]$ tel que $\left|q - \frac{x}{y}\right| < 1$:

On pose $\frac{x}{y} = \alpha + i\sqrt{2}\beta$ avec $\alpha, \beta \in \mathbb{R}$. Soient u et v les entiers les plus proches de α et β respectivement. On a

$$|u - \alpha| \leq 1/2 \text{ et } |v - \beta| \leq 1/2.$$

Scanned with CamScanner

Alors, pour $q = u + iv\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$, on a

$$\left|q - \frac{x}{y}\right|^2 = \left|(u-\alpha) + (v-\beta)i\sqrt{2}\right|^2 = (u-\alpha)^2 + 2(v-\beta)^2 \leq 1/4 + 2.1/4 = 3/4 < 1.$$

Donc,

$$\left|q - \frac{x}{y}\right| < 1.$$

(b) On pose $r = x - qy$. Vérifions que $|r| < |y|$:
On a

$$|r| = |x - qy| = |y|\left|\frac{x}{y} - q\right| < |y|.$$

(c) Montrons que l'anneau $\mathbb{Z}[i\sqrt{2}]$ est Euclidien :

— L'anneau $\mathbb{Z}[i\sqrt{2}]$ est intègre (car c'est un sous anneau du corps $\mathbb{C}$).
— On considère l'application $N : \mathbb{Z}[i\sqrt{2}]^* \to \mathbb{N}$ définie par $N(a + ib\sqrt{2}) = |a + ib|^2 = a^2 + 2b^2$ avec $a, b \in \mathbb{Z}$.
  — Soient $x, y \in \mathbb{Z}[i]^*$ tels que y divise x. Donc, il existe $z \in \mathbb{Z}[i]^*$ tel que $x = yz$. Comme $z \neq 0$ on a $N(z) \geq 1$. Donc, $N(x) = N(yz) = N(y)N(z) \geq N(y)$.
  — Soient $x, y \in \mathbb{Z}[i]$ avec $y \neq 0$. D'après ce qui précède, il existe $q, r \in \mathbb{Z}[i\sqrt{2}]$ tel que $x = qy + r$ avec $r = 0$ ou $N(r) < N(y)$.

Ceci montre que $\mathbb{Z}[i\sqrt{2}]$ est euclidien.

(5) Les diviseurs de $2 + i\sqrt{2}$ dans $\mathbb{Z}[i\sqrt{2}]$:
Soit $x = a + ib\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ un diviseur de $2 + i\sqrt{2}$ dans $\mathbb{Z}[i\sqrt{2}]$. Il existe $y \in \mathbb{Z}[i\sqrt{2}]$ tel que $2 + i\sqrt{2} = xy$. Donc, $6 = N(2 + i\sqrt{2}) = N(x)N(y)$. Ainsi, $N(x) \in \{1, 2, 3, 6\}$.
— Si $N(x) = 1$ alors $x = \pm 1$.
— Si $N(x) = 2$ alors $a^2 + 2b^2 = 2$. Donc, $a^2 = 0$ et $b^2 = 1$. Alors, $x = \pm\sqrt{2}i$. Inversement $\sqrt{2}i$ et $-\sqrt{2}i$ sont des diviseurs de $2 + i\sqrt{2}$. En effet,

$$2 + i\sqrt{2} = \sqrt{2}i(1 - \sqrt{2}i) = -\sqrt{2}i(-1 + \sqrt{2}i).$$

— Si $N(x) = 3$ alors $N(y) = 2$. Donc, $y = \pm\sqrt{2}i$. Par suite, $x = \pm(1 - \sqrt{2}i)$.
— Si $N(x) = 6$ alors $N(y) = 1$. Donc, $y = \pm 1$ et $x = \pm(2 + i\sqrt{2})$.
On conclut donc que les diviseurs de $2 + i\sqrt{2}$ sont exactement :

$$\pm 1, \quad \pm\sqrt{2}i, \quad \pm(1 - \sqrt{2}i), \quad \pm(2 + i\sqrt{2}).$$

(6) La liste des diviseurs communs de $2 + i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$:
Soit $x = a + ib\sqrt{2} \in \mathbb{Z}[i\sqrt{2}]$ un diviseur de 3 dans $\mathbb{Z}[i\sqrt{2}]$. Il existe $y \in \mathbb{Z}[i\sqrt{2}]$ tel que $3 = xy$. Donc, $9 = N(3) = N(x)N(y)$. Ainsi, $N(x) \in \{1, 3, 9\}$.
Les seuls diviseur de $2 + i\sqrt{2}$ qui vérifient cette condition sont : ± 1 et $\pm(1 - \sqrt{2}i)$. Il est clair que ± 1 divisent 3.Aussi, $3 = (1 - \sqrt{2}i)(1 + \sqrt{2}i)$. Donc, $\pm(1 - \sqrt{2}i)$ divisent aussi 3. Par conséquent, les diviseurs communs de $2 + i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$ sont exactement : ± 1 et $\pm(1 - \sqrt{2}i)$.

(7) Donner tous les pgcd de $2 + i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$: D'après la question précédente, les pgcd de $2 + i\sqrt{2}$ et 3 dans $\mathbb{Z}[i\sqrt{2}]$ sont $\pm(1 - \sqrt{2}i)$.

Exercice 5. On définit la norme de $z = x + yi \in \mathbb{C}$ par $N(z) = z\bar{z} = x^2 + y^2$.

Scanned with CamScanner

(1) Soit p un nombre premier. Montrer que les assertions suivantes sont équivalentes :
   (a) p est irréductible dans $\mathbb{Z}[i]$.
   (b) $p \equiv 3\,[4]$.
   (c) il n'existe pas $a \in \mathbb{Z}[i]$ tel que $p = N(a)$.
   On admettra que —1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ si et seulement si p n'est pas congru à 3 modulo 4.

(2) En déduire tous les irréductibles de $\mathbb{Z}[i]$.

(3) Parmi les éléments $1+i, 2+i, 2, 3, 5 \in \mathbb{Z}[i]$ lesquels sont irréductibles dans $\mathbb{Z}[i]$?

Solution.

(1) $(a) \Rightarrow (b)$. Supposons (a) et montrons (b) en raisonnant par l'absurde. Si $p \not\equiv 3\,[4]$, alors -1 est un carré dans $\mathbb{Z}/p\mathbb{Z}$ et il existe $x \in \mathbb{Z}$ tel que $-1 = x^2\,[p]$. On obtient alors que p divise $x^2+1 = (x+i)(x-i)$ dans $\mathbb{Z}[i]$. Puisque p est irréductible, il est donc un élément premier car $\mathbb{Z}[i]$ est euclidien. Donc, p divise $x+i$ ou $x-i$. Dans le premier cas $x+i = p(a+ib)$ pour $a, b \in \mathbb{Z}$. Ainsi, $1 = pa = pb$ ce qu'est absurde. Donc, p ne divise pas $x+i$. De même p ne divise pas $x-i$, ce qu'est absurde. Par conséquent, $p \equiv 3\,[4]$.
$(b) \Rightarrow (c)$. Supposons (b) et montrons (c), toujours par l'absurde. Si $p = N(x)$. Alors $p = u^2+v^2$, où u et v sont deux entiers tels que $x = u+iv$. Mais un carré étant toujours congru à 0 ou 1 (mod 4). Donc, p est congru à 0,1 ou 2 (mod 4), ce qui contredit (b). Par conséquent, il n'existe pas $x \in \mathbb{Z}[i]$ tel que $p = N(x)$.
$(c) \Rightarrow (a)$. Supposons (c) et démontrons (a). Soit a et b dans $\mathbb{Z}[i]$ tels que $p = ab$. On a $p^2 = N(p) = N(a)N(b)$. Si ni a ni b ne sont inversibles, on a $N(a)$ et $N(b)$ différents de 1. On obtient, puisque p est premier, $N(a) = N(b) = p$, ce qui contredit l'hypothèse. On conclut que a ou b est inversible, et donc p est irréductible.

(2) Les irréductibles de $\mathbb{Z}[i]$:
D'après les questions précédentes, les entiers premiers congrus à 3 modulo 4 sont irréductibles dans $\mathbb{Z}[i]$. Aussi, d'après la question (2) de l'exercice 1, les éléments a de $\mathbb{Z}[i]$ tels que $N(a)$ soit premier sont irréductibles.
On sait aussi que $U\big(\mathbb{Z}[i]\big) = \{\pm 1, \pm i\}$. Donc, si p est un entier premier congrus à 3 modulo 4 alors $\pm p$ et $\pm ip$ sont irréductibles (car ils sont associés à un élément irréductible) et si a de $\mathbb{Z}[i]$ tel que $N(a)$ soit premier alors $\pm a$ et $\pm ia$ sont irréductibles (car ils sont associés à un élément irréductible).

Montrons que ce sont les seuls éléments irréductibles de $\mathbb{Z}[i]$.
Soit x un élément irréductible de $\mathbb{Z}[i]$. On remarque que x divise $N(x) = x\overline{x} > 1$. L'entier $N(x)$ est un produit d'entiers premiers. Puisque x est irréductible (et donc premier car $\mathbb{Z}[i]$ est principal), il divise (dans $\mathbb{Z}[i]$) un de ces entiers premiers, appelons le p. Il existe $y \in \mathbb{Z}[i]$ tel que $p = xy$ et donc $p^2 = N(x)N(y)$. Si y est inversible, x est associé à p et nécessairement p est congru à 3 modulo 4, d'après la question 5. Sinon, on a, puisque $N(x) > 1$, $N(x) = p$ et x est un irréductible du type étudié dans l'exercice 1.

(3) Parmi les éléments $1+i, 2+i, 2, 3, 5 \in \mathbb{Z}[i]$ lesquels sont irréductibles dans $\mathbb{Z}[i]$?

— On a $N(1+i) = 2$ et $N(2+i) = 5$ sont premiers. Donc, $1+i$ et $2+i$ sont irréductibles.
— On a $2 \equiv 2\,[4]$, $3 \equiv 3\,[4]$ et $5 \equiv 1\,[4]$. Donc, 3 est irréductible dans $\mathbb{Z}[i]$ mais ni 2 ni 5 ne sont irréductibles dans $Z[i]$.

Scanned with CamScanner